

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2005 年 3 月 17 日 (17.03.2005)

PCT

(10) 国際公開番号
WO 2005/025126 A1

(51) 国際特許分類:
H04K 1/00, H04Q 7/38, H04M 1/725

H04L 9/08,

(71) 出願人 (米国を除く全ての指定国について): 学校法人同志社 (THE DOSHISHA) [JP/JP]; 〒6028580 京都府京都市上京区今出川通烏丸東入玄武町 6 0 1 番地 Kyoto (JP). 株式会社国際電気通信基礎技術研究所 (ADVANCED TELECOMMUNICATIONS RESEARCH INSTITUTE INTERNATIONAL) [JP/JP]; 〒6190288 京都府相楽郡精華町光台二丁目 2 番地 2 Kyoto (JP).

(21) 国際出願番号: PCT/JP2004/002228

(22) 国際出願日: 2004 年 2 月 25 日 (25.02.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-312156 2003 年 9 月 4 日 (04.09.2003) JP
特願2004-000533 2004 年 1 月 5 日 (05.01.2004) JP

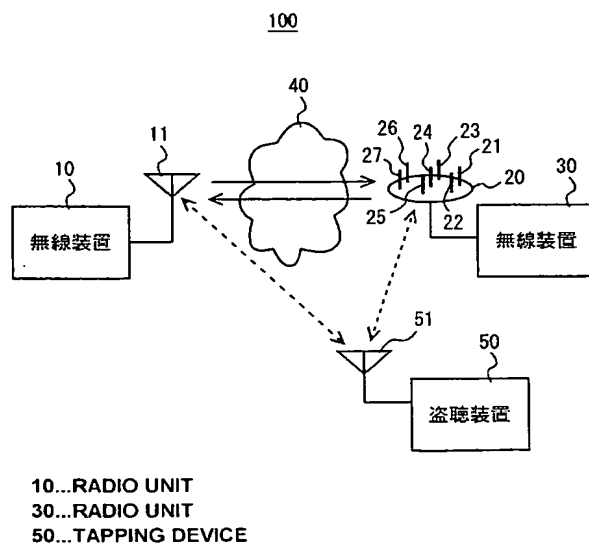
(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 笹岡 秀一 (SASAKA, Hideichi) [JP/JP]; 〒6100394 京都府京田辺市多々羅都谷 1-3 同志社大学内 Kyoto (JP). 青野 智之 (AONO, Tomoyuki) [JP/JP]; 〒6190288 京都府相楽郡精華町光台二丁目 2 番地 2 株式会社国際電気

[続葉有]

(54) Title: RADIO COMMUNICATION SYSTEM

(54) 発明の名称: 無線通信システム



(57) Abstract: A radio communication system (100) comprising radio units (10, 30), an antenna (11), and an array antenna (20). The radio units (10, 30) transmit/receive specified signals through the antenna (11) and the array antenna (20) at the same frequency by a time division duplex (TDD) transmission/reception system, for example, while varying the directivity of the array antenna (20) among a plurality of directivities. The radio units (10, 30) detect the intensity of a plurality of received radio waves and create receiving signal profiles (RSSI1, RSSI2) indicative of a plurality of intensity profiles. The radio units (10, 30) represent the plurality of intensities of the receiving signal profiles (RSSI1, RSSI2) in multi-values and create private keys (Ks1, Ks2) having a bit pattern of the plurality of multi-values.

(57) 要約: 無線通信システム (100) は、無線装置 (10, 30) と、アンテナ (11) と、アレーアンテナ (20) とを備える。無線装置 (10 及び 30) は、アレーアンテナ (20) の指向性を複数個に変えながら時分割復信 (TDD)

[続葉有]

WO 2005/025126 A1



通信基礎技術研究所内 Kyoto (JP). 大平 孝 (OHIRA, Takashi) [JP/JP]; 〒6190288 京都府相楽郡精華町光台二丁目2番地2 株式会社国際電気通信基礎技術研究所内 Kyoto (JP).

(74) 代理人: 深見 久郎, 外 (FUKAMI, Hisao et al.); 〒5300054 大阪府大阪市北区南森町2丁目1番29号 三井住友銀行南森町ビル 深見特許事務所 Osaka (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NL, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE,

SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書.

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

）等の同一周波数にて総受信する方式により所定の信号をアンテナ（11）及びアレーアンテナ（20）を介して相互に送受信する。そして、無線装置（10及び30）は、受信した複数の電波の強度を検出して複数の強度のプロファイルを示す受信信号プロファイル（RSSI1, RSSI2）をそれぞれ作成する。無線装置（10及び30）は、それぞれ、受信信号プロファイル（RSSI1, RSSI2）の複数の強度を多値化し、その多値化した複数の値をビットパターンとする秘密鍵（Ks1, Ks2）を作成する。

明細書

無線通信システム

5 技術分野

この発明は、無線通信システムに関し、特に、暗号化した情報を無線により通信する無線通信システムに関するものである。

背景技術

10 最近、情報化社会の発展に伴い情報通信が益々重要になるとともに、情報の盗聴または不正利用がより深刻な問題となっている。このような情報の盗聴を防止するために従来から情報を暗号化して送信することが行なわれている。

情報を暗号化して端末間で通信を行なう方式として公開鍵暗号方式と秘密鍵暗号方式とがある。公開鍵暗号方式は、安全性が高いが、大容量のデータの暗号化
15 には向かない。

一方、秘密鍵暗号方式は、処理が比較的簡単であり、大容量のデータの高速暗号化も可能であるが、秘密鍵を通信の相手方に送信する必要がある。また、秘密鍵暗号方式は、同一の秘密鍵を使用し続けると、暗号解読の攻撃を受けやすく、安全性が損なわれる可能性がある。

20 そこで、秘密鍵を相手方に送信せずに秘密鍵を共有する方法として、2つの端末間の伝送路の特性を測定し、その測定した特性に基づいて各端末で秘密鍵を生成する方法が提案されている（堀池 元樹、笹岡 秀一、「陸上移動通信路の不規則変動に基づく秘密鍵共有方式」、信学技報、社団法人 電子情報通信学会、2002年10月、TECHNICAL REPORT OF IEICE RCS2002-173, p. 7-12）。

25 この方法は、2つの端末間でデータを送受信したときの遅延プロファイルを各端末で測定し、その測定した遅延プロファイルをアナログ信号からデジタル信号に変換して各端末で秘密鍵を生成する方法である。即ち、伝送路を伝搬する電波は可逆性を示すために、一方の端末から他方の端末へデータを送信したときの遅延プロファイルは、他方の端末から一方の端末へ同じデータを送信したときの遅

延プロファイルと同じになる。従って、一方の端末で測定した遅延プロファイルに基づいて生成された秘密鍵は、他方の端末で測定した遅延プロファイルに基づいて作成された秘密鍵と同じになる。

5 このように、伝送路特性を用いて秘密鍵を生成する方法は、同じデータを2つの端末間で相互に送信するだけで同じ秘密鍵を共有することができる。

しかし、2つの端末間で送信されるデータを盗聴者が各端末の近傍で傍受して遅延プロファイルを測定すれば、盗聴者は、各端末で測定した遅延プロファイルに近い遅延プロファイルを取得することができる。その結果、秘密鍵が解読される可能性がある。

10 それゆえに、この発明の目的は、秘密鍵の盗聴を抑制可能な無線通信システムを提供することである。

発明の開示

この発明によれば、無線通信システムは、第1及び第2のアンテナと、第1及び第2の無線装置とを備える。第1のアンテナは、指向性を電氣的に切換え可能である。第1及び第2の無線装置は、第1及び第2のアンテナを介して無線伝送路により電波を相互に送受信する。そして、第1の無線装置は、第1のアンテナの指向性が所定のパターンにより複数個に変えられたときに第2の無線装置から受信した複数の電波に基づいて複数の電波の強度プロファイルを示す第1の受信信号プロファイルを生成し、その生成した第1の受信信号プロファイルに基づいて第1の秘密鍵を生成する。また、第2の無線装置は、第1のアンテナの指向性が所定のパターンにより複数個に変えられたときに第1の無線装置から受信した複数の電波に基づいて複数の電波の強度プロファイルを示す第2の受信信号プロファイルを生成し、その生成した第2の受信信号プロファイルに基づいて第1の秘密鍵と同じ第2の秘密鍵を生成する。

好ましくは、第1及び第2の受信信号プロファイルの各々は、複数個の指向性に対応した複数の強度からなる。第1及び第2の無線装置は、複数の強度を多値化してそれぞれ第1及び第2の秘密鍵を生成する。

好ましくは、第1及び第2の無線装置は、時分割復信方式により複数の電波を

送受信する。

好ましくは、第１の無線装置は、生成した第１の秘密鍵が第２の秘密鍵に一致することを確認する。

また、この発明によれば、無線通信システムは、第１および第２のアンテナと、
5 第１および第２の無線装置とを備える。第１のアンテナは、指向性を電氣的に切
換え可能なアンテナである。第１および第２の無線装置は、第１及び第２のアン
テナを介して無線伝送路により電波を相互に送受信する。そして、第１の無線装
置は、第１のアンテナの指向性が所定のパターンにより複数個に変えられたとき
10 に第２の無線装置が所定の通信プロトコルに従って送信した複数のデータに対応
する複数の電波を受信し、その受信した複数の電波に基づいて複数の電波の強度
プロファイルを示す第１の受信信号プロファイルを生成し、その生成した第１の
受信信号プロファイルに基づいて第１の秘密鍵を生成する。また、第２の無線装
置は、第１のアンテナの指向性が所定のパターンにより複数個に変えられたとき
15 に第１の無線装置が所定の通信プロトコルに従って送信した複数のデータに対応
する複数の電波を受信し、その受信した複数の電波に基づいて複数の電波の強度
プロファイルを示す第２の受信信号プロファイルを生成し、その生成した第２の
受信信号プロファイルに基づいて第１の秘密鍵と同じ第２の秘密鍵を生成する。

好ましくは、第１の無線装置は、第１のアンテナが無指向性に制御されたとき
に第２の無線装置との間で無線伝送路を確立し、無線伝送路が確立した後、第１
20 のアンテナの指向性を複数個に変えながら第２の無線装置との間で複数のデータ
を送受信する。

好ましくは、第１の無線装置は、第２の無線装置との間における各データの送
受信において、第１のアンテナの指向性を更新して第２の無線装置からデータを
受信し、更新した第１のアンテナの指向性を維持して受信したデータを第２の無
25 線装置へ送信する。

好ましくは、所定の通信プロトコルは、複数の階層からなる。複数のデータは、
複数の階層のうち、データを電気信号に変換する階層におけるデータフォーマッ
トに含まれる。そして、データを電気信号に変換する階層は、複数の通信プロト
コルに共通な階層である。

好ましくは、複数のデータの各々は、第1および第2の無線装置により受信された電波の強度を検出する区間と、第1のアンテナの指向性を変更する区間とからなる。

好ましくは、第1の無線装置は、生成した第1の秘密鍵が第2の秘密鍵に不一致であるとき、第1の秘密鍵を第2の秘密鍵に一致させる。

好ましくは、第1のアンテナは、盗聴者の端末に近接して配置された第1の無線装置に設置される。

好ましくは、第1及び第2の無線装置は、第1及び第2の秘密鍵を用いてデータを暗号及び復号して相互に通信する。

この発明による無線通信システムにおいては、指向性を電氣的に切換え可能な第1のアンテナを介して2つの無線装置間で所定のデータが送受信される。そして、第1のアンテナの指向性を複数個に変えたときに検出される複数の電波の強度プロファイルを示す受信信号プロファイルが2つの無線装置において生成され、その生成された各受信信号プロファイルに基づいて2つの無線装置において秘密鍵が作成される。この場合、各無線装置において生成される受信信号プロファイルは、2つの無線装置間に形成される伝送路に固有である。即ち、2つの無線装置間で送受信される複数の電波を傍受して受信信号プロファイルを生成しても、その生成した受信信号プロファイルは、2つの端末装置で生成される受信信号プロファイルと異なる。

従って、この発明によれば、2つの無線装置において作成される秘密鍵の盗聴を抑制できる。

また、この発明による無線通信システムにおいては、指向性を電氣的に切換え可能なアンテナを介して2つの無線装置間で所定のデータが所定の通信プロトコルに従って送受信される。そして、このアンテナの指向性を複数個に変えたときに検出される複数の電波の強度プロファイルを示す受信信号プロファイルが2つの無線装置において生成され、その生成された各受信信号プロファイルに基づいて2つの無線装置において秘密鍵が作成される。この場合、各無線装置において生成される受信信号プロファイルは、2つの無線装置間に形成される伝送路に固有である。即ち、2つの無線装置間で送受信される複数の電波を傍受して受信信

号プロファイルを生成しても、その生成した受信信号プロファイルは、2つの端末装置で生成される受信信号プロファイルと異なる。

従って、この発明によれば、2つの無線装置において作成される秘密鍵の盗聴を抑制できる。また、2つの無線装置において作成される秘密鍵を生成するためのデータを所定の通信プロトコルに従って送受信できる。

図面の簡単な説明

図1は、この発明の実施の形態1による無線通信システムの概略図である。

図2は、図1に示す一方の無線装置の概略ブロック図である。

図3は、図1に示す他方の無線装置の概略ブロック図である。

図4は、図3に示す指向性設定部の概略ブロック図である。

図5は、図2及び図3に示す鍵一致確認部の概略ブロック図である。

図6は、図2及び図3に示す鍵一致化部の概略ブロック図である。

図7は、受信信号プロファイルRSSIの概念図である。

図8は、図1に示す2つの無線装置間で通信を行なう動作を説明するためのフローチャートである。

図9は、実施の形態2による無線通信システムの概略図である。

図10は、図9に示す一方の無線装置の内部構成を示す概略ブロック図である。

図11は、図9に示す他方の無線装置の内部構成を示す概略ブロック図である。

図12は、図11に示す指向性設定部の機能ブロック図である。

図13は、所定の通信プロトコルであるIEEE802.11b（またはIEEE802.11g）の物理層およびMAC層のフォーマットを示す図である。

図14は、2つの無線装置間でデータを送受信する通常の方法の概念図である。

図15は、2つの無線装置間におけるデータの再送の概念図である。

図16は、実施の形態2において、2つの無線装置間でデータを送受信する方法の概念図である。

図17は、図9に示す2つの無線装置間で通信を行なう動作を説明するためのフローチャートである。

発明を実施するための最良の形態

本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

〔実施の形態１〕

5 図１は、この発明の実施の形態１による無線通信システムの概略図である。無線通信システム１００は、無線装置１０、３０と、アンテナ１１と、アレーアンテナ２０とを備える。無線装置１０は、例えば、ユーザの移動体通信端末である。また、無線装置３０は、例えば、無線アクセスポイントである。

10 アンテナ１１は、無線装置１０に装着される。そして、アンテナ１１は、全方位性のアンテナである。アレーアンテナ２０は、アンテナ素子２１～２７を備える。アンテナ素子２４は、給電素子であり、アンテナ素子２１～２３、２５～２７は、無給電素子である。そして、アンテナ素子２４は、アンテナ素子２１～２３、２５～２７によって取り囲まれている。無給電素子であるアンテナ素子２１～２３、２５～２７に装荷された可変容量素子であるバラクタダイオードに印加する直流電圧を制御することにより、アレーアンテナ２０は、適応ビーム形成が
15 可能である。

即ち、アレーアンテナ２０は、無線装置３０に含まれるバラクタダイオード（図示せず）に印加する直流電圧を変えることによって指向性を変えられる。従って、アレーアンテナ２０は、電氣的に指向性を切換え可能なアンテナである。
20 そして、アレーアンテナ２０は、無線装置３０に装着される。

無線装置１０と無線装置３０との間で通信が行われる場合、電波は、無線装置１０のアンテナ１１と無線装置３０のアレーアンテナ２０との間を直接伝搬したり、中間物４０による影響を受けて伝搬する。中間物４０としては、反射物及び障害物が想定される。中間物４０が反射物である場合、無線装置１０のアンテナ
25 １１または無線装置３０のアレーアンテナ２０から出射した電波は、中間物４０によって反射されて無線装置３０のアレーアンテナ２０または無線装置１０のアンテナ１１へ伝搬する。また、中間物４０が障害物である場合、無線装置１０のアンテナ１１または無線装置３０のアレーアンテナ２０から出射した電波は、中間物４０によって回折されて無線装置３０のアレーアンテナ２０または無線装置

10のアンテナ11へ伝搬する。

このように、電波は、無線装置10のアンテナ11と無線装置30のアレーアンテナ20との間を直接伝搬したり、中間物40による反射を受けて反射波として伝搬したり、中間物40による回折を受けて回折波として伝搬したりする。そして、電波は、無線装置10のアンテナ11または無線装置30のアレーアンテナ20から無線装置30のアレーアンテナ20または無線装置10のアンテナ11へ伝搬する場合、直接伝搬成分、反射波成分及び回折波成分が混在しており、無線装置10のアンテナ11または無線装置30のアレーアンテナ20から無線装置30のアレーアンテナ20または無線装置10のアンテナ11へ伝搬した電波がどのような成分により構成されるかによって無線装置10と無線装置30との間の伝送路の特性が決定される。

この発明においては、無線装置10と無線装置30との間で通信が行なわれる場合、アレーアンテナ20の指向性を複数個に変えて時分割復信（TDD：Time Division Duplex）等の同一周波数で送受信する方式で所定のデータが無線装置10、30間で送受信される。そして、無線装置10、30は、アレーアンテナ20の指向性を複数個に変えたときの複数の電波の強度を示す受信信号プロファイルRSSIを生成し、その生成した受信信号プロファイルRSSIに基づいて秘密鍵を作成する。

秘密鍵が無線装置10、30において生成されると、無線装置10、30は、生成した秘密鍵により情報を暗号化して相手方へ送信し、相手方から受信した暗号化情報を復号して情報を取得する。

図2は、図1に示す一方の無線装置10の概略ブロック図である。無線装置10は、信号発生部110と、送信処理部120と、アンテナ部130と、受信処理部140と、プロファイル生成部150と、鍵作成部160と、鍵一致確認部170と、鍵記憶部180と、鍵一致化部190と、暗号部200と、復号部210とを含む。

信号発生部110は、秘密鍵を生成するときに無線装置30へ送信するための所定の信号を生成し、その生成した所定の信号を送信処理部120へ出力する。送信処理部120は、変調、周波数変換、多元接続及び送信信号の増幅等の送信

系の処理を行なう。アンテナ部 130 は、図 1 に示すアンテナ 11 からなり、送信処理部 120 からの信号を無線装置 30 へ送信し、無線装置 30 からの信号を受信して受信処理部 140 またはプロファイル生成部 150 へ供給する。

5 受信処理部 140 は、受信信号の増幅、多元接続、周波数変換及び復調等の受信系の処理を行なう。そして、受信処理部 140 は、受信処理を行なった信号を必要に応じて鍵一致確認部 170、鍵一致化部 190 及び復号部 210 へ出力する。

10 プロファイル生成部 150 は、アレーアンテナ 20 の指向性を複数個に変えたときの複数の電波をアンテナ部 130 から順次受け、その受けた複数の電波の強度を検出する。そして、プロファイル生成部 150 は、検出した複数の強度からなる受信信号プロファイル RSSI を生成して鍵作成部 160 へ出力する。

鍵作成部 160 は、プロファイル生成部 150 からの受信信号プロファイル RSSI に基づいて秘密鍵 Ks1 を作成する。そして、鍵作成部 160 は、作成した秘密鍵 Ks1 を鍵一致確認部 170 及び鍵一致化部 190 へ出力する。

15 鍵一致確認部 170 は、所定の信号を送信処理部 120、アンテナ部 130 及び受信処理部 140 を介して無線装置 30 と送受信し、鍵作成部 160 によって作成された秘密鍵 Ks1 が無線装置 30 において作成された秘密鍵 Ks2 に一致するか否かを後述する方法によって確認する。そして、鍵一致確認部 170 は、秘密鍵 Ks1 が秘密鍵 Ks2 に一致すると確認したとき、秘密鍵 Ks1 を鍵記憶部 180 に記憶する。また、鍵一致確認部 170 は、秘密鍵 Ks1 が秘密鍵 Ks2 に不一致であることを確認したとき、不一致信号 NMTH を生成して鍵一致化部 190 へ出力する。

20 鍵記憶部 180 は、鍵一致確認部 170 及び鍵一致化部 190 からの秘密鍵 Ks1 を記憶する。また、鍵記憶部 180 は、記憶した秘密鍵 Ks1 を暗号部 200 及び復号部 210 へ出力する。なお、鍵記憶部 180 は、秘密鍵 Ks1 を一時的、例えば、無線装置 30 との通信の間だけ記憶するようにしてもよい。

鍵一致化部 190 は、鍵一致確認部 170 から不一致信号 NMTH を受けると、後述する方法によって秘密鍵 Ks1 を秘密鍵 Ks2 に一致させる。そして、鍵一致化部 190 は、一致させた秘密鍵が秘密鍵 Ks2 に一致することを鍵一致確認

部 1 7 0 における方法と同じ方法によって確認する。

暗号部 2 0 0 は、送信データを鍵記憶部 1 8 0 に記憶された秘密鍵 $K_s 1$ によって暗号して送信処理部 1 2 0 へ出力する。復号部 2 1 0 は、受信処理部 1 4 0 からの信号を鍵記憶部 1 8 0 からの秘密鍵 $K_s 1$ によって復号して受信データを生成する。

図 3 は、図 1 に示す他方の無線装置 3 0 の概略ブロック図である。無線装置 3 0 は、無線装置 1 0 のアンテナ部 1 3 0 をアンテナ部 2 2 0 に代え、指向性設定部 2 3 0 を追加したものであり、その他は、無線装置 1 0 と同じである。

アンテナ部 2 2 0 は、図 1 に示すアレーアンテナ 2 0 からなる。そして、アンテナ部 2 2 0 は、送信処理部 1 2 0 からの信号を指向性設定部 2 3 0 によって設定された指向性で無線装置 1 0 へ送信し、無線装置 1 0 からの信号を指向性設定部 2 3 0 によって設定された指向性で受信して受信処理部 1 4 0 またはプロフィール生成部 1 5 0 へ出力する。

指向性設定部 2 3 0 は、アンテナ部 2 2 0 の指向性を設定する。また、指向性設定部 2 3 0 は、無線装置 1 0、3 0 において秘密鍵 $K_s 1$ 、 $K_s 2$ を生成するとき、後述する方法により所定の順序に従ってアンテナ部 2 2 0 の指向性を順次切替える。

なお、無線装置 3 0 のプロフィール生成部 1 5 0 は、アレーアンテナ 2 0 の指向性を複数個に変えたときの複数の電波をアンテナ部 2 2 0 から順次受け、その受けた複数の電波の強度を検出する。そして、プロフィール生成部 1 5 0 は、検出した複数の強度からなる受信信号プロフィール $RSSI$ を生成して鍵作成部 1 6 0 へ出力する。

図 4 は、図 3 に示す指向性設定部 2 3 0 の概略ブロック図である。指向性設定部 2 3 0 は、制御電圧発生回路 2 3 1 と、バラクタダイオード 2 3 2 とを含む。制御電圧発生回路 2 3 1 は、制御電圧セット $CLV 1 \sim CLV n$ (n は自然数) を順次発生し、その発生した制御電圧セット $CLV 1 \sim CLV n$ をバラクタダイオード 2 3 2 へ順次出力する。バラクタダイオード 2 3 2 は、制御電圧セット $CLV 1 \sim CLV n$ に応じて無給電素子であるアンテナ素子 2 1 \sim 2 3、2 5 \sim 2 7 に装荷される容量を変え、アレーアンテナ 2 0 の指向性を複数個に順次変える。

図5は、図2及び図3に示す鍵一致確認部170の概略ブロック図である。鍵一致確認部170は、データ発生部171と、データ比較部172と、結果処理部173とを含む。なお、無線装置10、30の鍵一致確認部170は、同じ構成からなるが、図5においては、秘密鍵Ks1が秘密鍵Ks2に一致することを
5 確認する動作を説明するために、無線装置30においてはデータ発生部171のみを示す。

データ発生部171は、鍵作成部160から秘密鍵Ks1を受けると、秘密鍵Ks1が秘密鍵Ks2に一致することを確認するための鍵確認用データDCFM1を発生し、その発生した鍵確認用データDCFM1を送信処理部120及びデ
10 ータ比較部172へ出力する。

この場合、データ発生部171は、秘密鍵Ks1から非可逆的な演算及び一方向的な演算等により、鍵確認用データDCFM1を発生する。より具体的には、データ発生部171は、秘密鍵Ks1またはKs2のハッシュ値を演算することにより、鍵確認用データDCFM1を発生する。

データ比較部172は、データ発生部171から鍵確認用データDCFM1を受け、無線装置30のデータ発生部171で発生された鍵確認用データDCFM2を受信処理部140から受ける。そして、データ比較部172は、鍵確認用データDCFM1を鍵確認用データDCFM2と比較する。データ比較部172は、
15 鍵確認用データDCFM1が鍵確認用データDCFM2に一致するとき、一致信号MTHを生成して結果処理部173へ出力する。

また、データ比較部172は、鍵確認用データDCFM1が鍵確認用データDCFM2に不一致であるとき、不一致信号NMTHを生成する。そして、データ比較部172は、不一致信号NMTHを鍵一致化部190へ出力し、不一致信号NMTHを送信処理部120及びアンテナ部130を介して無線装置30へ送信
20 する。

結果処理部173は、データ比較部172から一致信号MTHを受けると、鍵作成部160から受けた秘密鍵Ks1を鍵記憶部180へ記憶する。

図6は、図2及び図3に示す鍵一致化部190の概略ブロック図である。鍵一致化部190は、擬似シンドローム作成部191と、不一致ビット検出部192

と、鍵不一致訂正部 193 と、データ発生部 194 と、データ比較部 195 と、結果処理部 196 とを含む。

5 なお、無線装置 10、30 の鍵一致化部 190 は、同じ構成からなるが、図 6 においては、秘密鍵 K_{s1} を秘密鍵 K_{s2} に一致させる動作を説明するために、無線装置 30 においては擬似シンδροーム作成部 191 のみを示す。

10 擬似シンδροーム作成部 191 は、鍵一致確認部 170 のデータ比較部 172 から不一致信号 NMTH を受けると、鍵作成部 160 から受けた秘密鍵 K_{s1} のシンδροーム x_1 を演算する。より具体的には、擬似シンδροーム作成部 191 は、秘密鍵 K_{s1} のビットパターン x_1 を検出し、ビットパターン x_1 に対して
10 検査行列 H を乗算してシンδροーム $s_1 = x_1 H^T$ を演算する。そして、擬似シンδροーム作成部 191 は、ビットパターン x_1 を鍵不一致訂正部 193 へ出力し、演算したシンδροーム $s_1 = x_1 H^T$ を不一致ビット検出部 192 へ出力する。

15 なお、これらの演算は、 $\text{mod } 2$ の演算であり、 H^T は、検査行列 H の転置行列である。

20 不一致ビット検出部 192 は、擬似シンδροーム作成部 191 からシンδροーム s_1 を受け、無線装置 30 の擬似シンδροーム作成部 191 によって演算されたシンδροーム $s_2 = x_2 H^T$ を受信処理部 140 から受ける。そして、不一致ビット検出部 192 は、シンδροーム s_1 とシンδροーム s_2 との差分 $s = s_1 - s_2$ を演算する。

25 なお、秘密鍵 K_{s1} 、 K_{s2} のビットパターンの差分（鍵不一致のビットパターン）を $e = x_1 - x_2$ とすると、 $s = e H^T$ の関係が成立する。 $s = 0$ の場合、 $e = 0$ となり、秘密鍵 K_{s1} のビットパターンは、秘密鍵 K_{s2} のビットパターンに一致する。

30 不一致ビット検出部 192 は、演算した差分 s が 0 でないとき（即ち、 $e \neq 0$ のとき）、鍵不一致のビットパターン e を鍵不一致訂正部 193 へ出力する。

35 鍵不一致訂正部 193 は、擬似シンδροーム作成部 191 からビットパターン x_1 を受け、不一致ビット検出部 192 から鍵不一致のビットパターン e を受ける。そして、鍵不一致訂正部 193 は、ビットパターン x_1 から鍵不一致のビッ

トパターン e を減算することにより相手方の秘密鍵のビットパターン $x_2 = x_1 - e$ を演算する。

このように、鍵一致化部190は、秘密鍵 K_{s1} 、 K_{s2} の不一致を誤りと見なして誤り訂正の応用により秘密鍵 K_{s1} 、 K_{s2} の不一致を解消する。

- 5 この秘密鍵を一致させる方法は、鍵不一致のビット数が誤り訂正能力以上である場合に鍵の一致化に失敗する可能性があるので、鍵一致化の動作を行なった後に鍵一致の確認を行なう必要がある。

10 データ発生部194は、一致化後の鍵 $x_2 = x_1 - e$ を鍵不一致訂正部193から受けると、鍵 x_2 に基づいて鍵確認用データDCFM3を発生させ、その発生させた鍵確認用データDCFM3をデータ比較部195へ出力する。また、データ発生部194は、発生させた鍵確認用データDCFM3を送信処理部120及びアンテナ部130を介して無線装置30へ送信する。

15 なお、データ発生部194は、鍵一致確認部170のデータ発生部171による鍵確認用データDCFM1の発生方法と同じ方法により鍵確認用データDCFM3を発生する。

データ比較部195は、データ発生部194から鍵確認用データDCFM3を受け、無線装置30で発生された鍵確認用データDCFM4を受信処理部140から受ける。そして、データ比較部195は、鍵確認用データDCFM3を鍵確認用データDCFM4と比較する。

20 データ比較部195は、鍵確認用データDCFM3が鍵確認用データDCFM4に一致するとき、一致信号MTHを生成して結果処理部196へ出力する。

25 また、データ比較部195は、鍵確認用データDCFM3が鍵確認用データDCFM4に不一致であるとき、不一致信号NMTHを生成する。そして、データ比較部195は、不一致信号NMTHを送信処理部120及びアンテナ部130を介して無線装置30へ送信する。

結果処理部196は、データ比較部195から一致信号MTHを受けると、鍵不一致訂正部193から受けた鍵 $x_2 = x_1 - e$ を鍵記憶部180へ記憶する。

このように、データ発生部194、データ比較部195及び結果処理部196は、鍵一致確認部170における確認方法と同じ方法によって一致化が施された

鍵の一致を確認する。

図7は、受信信号プロファイルRSSIの概念図である。指向性設定部230の制御電圧発生回路231は、各々が電圧V1～V6からなる制御電圧セットCLV1～CLVnを順次発生してバラクタダイオード232へ出力する。この場合、電圧V1～V6は、それぞれ、アンテナ素子21～23, 25～27に装荷される容量を変えるための電圧であり、0～20Vの範囲で変えられる。

バラクタダイオード232は、パターンP1からなる制御電圧セットCLV1に応じてアレーアンテナ20の指向性のある1つの指向性に設定する。そして、アレーアンテナ20は、設定された指向性で無線装置10からの電波を受信してプロファイル生成部150へ供給する。プロファイル生成部150は、アレーアンテナ20（アンテナ部220）から受けた電波の強度WI1を検出する。

次に、バラクタダイオード232は、パターンP2からなる制御電圧セットCLV2に応じてアレーアンテナ20の指向性を別の指向性に設定する。そして、アレーアンテナ20は、設定された指向性で無線装置10からの電波を受信してプロファイル生成部150へ供給する。プロファイル生成部150は、アレーアンテナ20（アンテナ部220）から受けた電波の強度WI2を検出する。

以後、同様にして、バラクタダイオード232は、それぞれ、パターンP3～Pnからなる制御電圧セットCLV3～CLVnに応じてアレーアンテナ20の指向性を順次変える。そして、アレーアンテナ20は、各々設定された指向性で無線装置10からの電波を受信してプロファイル生成部150へ供給する。プロファイル生成部150は、アレーアンテナ20（アンテナ部220）から受けた電波の強度WI3～WINを順次検出する。

そして、プロファイル生成部150は、強度WI1～WINからなる強度プロファイルを示す受信信号プロファイルRSSIを生成して鍵作成部160へ出力する。

パターンP1～Pnによってアレーアンテナ20の指向性を複数個に順次切換えて無線装置30から無線装置10へデータを送信したとき、無線装置10のプロファイル生成部150が受信信号プロファイルRSSIを生成する。

鍵作成部160は、プロファイル生成部150から受信信号プロファイルRS

5 S Iを受け、受信信号プロファイルRSSIから最大強度 WI_{max} ($=WI_6$)を検出する。そして、鍵作成部160は、最大強度 WI_{max} ($=WI_6$)によって受信信号プロファイルRSSIを規格化し、各強度 $WI_1 \sim WI_n$ を多値化する。鍵作成部160は、多値化した各値を検出し、その検出した各値をビットパターンとする秘密鍵 K_{s1} または K_{s2} を作成する。

10 図8は、図1に示す2つの無線装置10、30間で通信を行なう動作を説明するためのフローチャートである。一連の動作が開始されると、無線装置30の送信処理部120は、 $k=1$ を設定する(ステップS1)。そして、指向性設定部230は、パターンP1によりアレーアンテナ20の指向性を1つの指向性に設定する(ステップS2)。

その後、無線装置10の信号発生部110は、所定の信号を発生して送信処理部120へ出力する。送信処理部120は、所定の信号に変調等の処理を施し、アンテナ11を介して無線装置30へ所定の信号を構成する電波を送信する(ステップS3)。

15 無線装置30において、アレーアンテナ20は、無線装置10からの電波を受信し、その受信した電波をプロファイル生成部150へ出力する。プロファイル生成部150は、アレーアンテナ20から受けた電波の強度 I_{1k} を検出する(ステップS4)。

20 その後、無線装置30の信号発生部110は、所定の信号を発生して送信処理部120へ出力する。送信処理部120は、所定の信号に変調等の処理を施し、アレーアンテナ20を介して無線装置10へ所定の信号を構成する電波を送信する(ステップS5)。

25 無線装置10において、アンテナ11は、無線装置30からの電波を受信し、その受信した電波をプロファイル生成部150へ出力する。プロファイル生成部150は、アンテナ11から受けた電波の強度 I_{2k} を検出する(ステップS6)。

その後、無線装置30の送信処理部120は、 $k=k+1$ を設定し(ステップS7)、 $k=n$ であるか否かを判定する(ステップS8)。そして、 $k=n$ でないとき、ステップS2～S8が繰返し実行される。即ち、アレーアンテナ20の

指向性がパターンP1～Pnによってn個に変えられて、無線装置10のアンテナ11と無線装置30のアレーアンテナ20との間で所定の信号を構成する電波が送受信され、強度I11～I1n及びI21～I2nが検出されるまで、ステップS2～S8が繰返し実行される。

- 5 ステップS8において、 $k=n$ であると判定されると、無線装置30において、プロファイル生成部150は、強度I11～I1nから受信信号プロファイルRSSI1を作成して鍵作成部160へ出力する。

10 鍵作成部160は、受信信号プロファイルRSSI1から最大強度 $W_{I_{max}1}$ を検出し、その検出した最大強度 $W_{I_{max}1}$ によって受信信号プロファイルRSSI1を規格化し、強度I11～I1nを多値化する。そして、鍵作成部160は、多値化した各値をビットパターンとする秘密鍵 K_{s2} を生成する（ステップS9）。

15 また、無線装置10のプロファイル生成部150は、強度I21～I2nから受信信号プロファイルRSSI2を作成して鍵作成部160へ出力する。鍵作成部160は、受信信号プロファイルRSSI2から最大強度 $W_{I_{max}2}$ を検出し、その検出した最大強度 $W_{I_{max}2}$ によって受信信号プロファイルRSSI2を規格化し、強度I21～I2nを多値化する。そして、鍵作成部160は、多値化した各値をビットパターンとする秘密鍵 K_{s1} を生成する（ステップS10）。

20 その後、無線装置10において、鍵作成部160は、秘密鍵 K_{s1} を鍵一致確認部170へ出力する。鍵一致確認部170のデータ発生部171は、上述した方法によって鍵確認用データDCFM1を発生して送信処理部120及びデータ比較部172へ出力する。送信処理部120は、鍵確認用データDCFM1に変調等の処理を施し、アンテナ部130を介して無線装置30へ鍵確認用データDCFM1を送信する。

25 そして、アンテナ部130は、無線装置30において発生された鍵確認用データDCFM2を無線装置30から受信し、その受信した鍵確認用データDCFM2を受信処理部140へ出力する。受信処理部140は、鍵確認用データDCFM2に所定の処理を施し、鍵一致確認部170のデータ比較部172へ鍵確認用

データDCFM2を出力する。

データ比較部172は、データ発生部171からの鍵確認用データDCFM1を受信処理部140からの鍵確認用データDCFM2と比較する。そして、データ比較部172は、鍵確認用データDCFM1が鍵確認用データDCFM2に一致しているとき、一致信号MTHを生成して結果処理部173へ出力する。結果処理部173は、一致信号MTHに応じて、鍵作成部160からの秘密鍵Ks1を鍵記憶部180に記憶する。

一方、鍵確認用データDCFM1が鍵確認用データDCFM2に不一致であるとき、データ比較部172は、不一致信号NMTHを生成して送信処理部120及び鍵一致化部190へ出力する。送信処理部120は、不一致信号NMTHをアンテナ部130を介して無線装置30へ送信する。そして、無線装置30は、無線装置10において秘密鍵Ks1、Ks2の不一致が確認されたことを検知する。

これにより、無線装置10における鍵一致の確認が終了する（ステップS11）。

なお、無線装置10における鍵一致確認に代えて、無線装置30において鍵一致確認をしてもよい（ステップS12）。

ステップS11において、秘密鍵Ks1、Ks2の不一致が確認されたとき、無線装置10において、鍵一致化部190の擬似シンδροーム作成部191は、鍵一致確認部170から不一致信号NMTHを受ける。そして、擬似シンδροーム作成部191は、不一致信号NMTHに応じて、鍵作成部160から受けた秘密鍵Ks1のビットパターン x_1 を検出し、その検出したビットパターン x_1 のシンδροーム $s_1 = x_1 H^T$ を演算する。

擬似シンδροーム作成部191は、演算したシンδροーム $s_1 = x_1 H^T$ を不一致ビット検出部192へ出力し、ビットパターン x_1 を鍵不一致訂正部193へ出力する。

一方、無線装置30は、ステップS11において無線装置10から不一致信号NMTHを受信し、その受信した不一致信号NMTHに応じて、シンδροーム $s_2 = x_2 H^T$ を演算して無線装置10へ送信する。

無線装置 10 のアンテナ部 130 は、無線装置 30 からシンドローム $s_2 = x_2 H^T$ を受信して受信処理部 140 へ出力する。受信処理部 140 は、シンドローム $s_2 = x_2 H^T$ に対して所定の処理を施し、シンドローム $s_2 = x_2 H^T$ を鍵一致化部 190 へ出力する。

- 5 鍵一致化部 190 の不一致ビット検出部 192 は、受信処理部 140 から無線装置 30 において作成されたシンドローム $s_2 = x_2 H^T$ を受ける。そして、不一致ビット検出部 192 は、無線装置 10 で作成されたシンドローム $s_1 = x_1 H^T$ と無線装置 30 において作成されたシンドローム $s_2 = x_2 H^T$ との差分 $s = s_1 - s_2$ を演算する。

- 10 その後、不一致ビット検出部 192 は、 $s \neq 0$ であることを確認し、鍵不一致のビットパターン $e = x_1 - x_2$ を $s = e H^T$ に基づいて演算し、その演算した鍵不一致のビットパターン e を鍵不一致訂正部 193 へ出力する。

- 15 鍵不一致訂正部 193 は、擬似シンドローム作成部 191 からのビットパターン x_1 と、不一致ビット検出部 192 からの鍵不一致のビットパターン e とに基づいて、無線装置 30 において作成された秘密鍵 K_{s_2} のビットパターン $x_2 = x_1 - e$ を演算する。

そして、データ発生部 194、データ比較部 195 及び結果処理部 196 は、鍵一致確認部 170 における鍵一致確認の動作と同じ動作によって、一致化された鍵 $x_2 = x_1 - e$ の一致を確認する。

- 20 これにより、鍵不一致対策が終了する（ステップ S13）。

なお、無線装置 10 における鍵不一致対策に代えて、無線装置 30 において鍵不一致対策をしてもよい（ステップ S14）。

- 25 ステップ S11 において、秘密鍵 K_{s_1} が秘密鍵 K_{s_2} に一致することが確認されたとき、またはステップ S13 において鍵不一致対策がなされたとき、暗号部 200 は、鍵記憶部 180 から秘密鍵 K_{s_1} を読出して送信データを暗号化し、暗号化した送信データを送信処理部 120 へ出力する。そして、送信処理部 120 は、暗号化された送信データに変調等を施し、アンテナ部 130 を介して暗号化された送信データを無線装置 30 へ送信する。

また、アンテナ部 130 は、暗号化された送信データを無線装置 30 から受信

し、その受信した暗号化された送信データを受信処理部 140 へ出力する。受信処理部 140 は、暗号化された送信データに所定の処理を施し、暗号化された送信データを復号部 210 へ出力する。

5 復号部 210 は、受信処理部 140 からの暗号化された送信データを復号して受信データを取得する。

これにより、秘密鍵 $K_s 1$ による暗号・復号が終了する（ステップ S 15）。

無線装置 30 においても、無線装置 10 と同じ動作によって秘密鍵 $K_s 2$ による暗号・復号が行なわれる（ステップ S 16）。そして、一連の動作が終了する。

10 上述したステップ S 3, S 4 に示す動作は、無線装置 30 において受信信号プロファイル $RSSI 1$ を生成するための電波を無線装置 10 のアンテナ 11 から無線装置 30 のアレーアンテナ 20 へ送信し、かつ、無線装置 30 において電波の強度 I_{1k} を検出する動作であり、ステップ S 5, S 6 に示す動作は、無線装置 10 において受信信号プロファイル $RSSI 2$ を生成するための電波を無線装置 30 のアレーアンテナ 20 から無線装置 10 のアンテナ 11 へ送信し、かつ、
15 無線装置 10 において電波の強度 I_{2k} を検出する動作である。そして、所定の信号を構成する電波の無線装置 10 のアンテナ 11 から無線装置 30 のアレーアンテナ 20 への送信及び所定の信号を構成する電波の無線装置 30 のアレーアンテナ 20 から無線装置 10 のアンテナ 11 への送信は、アレーアンテナ 20 の指向性を 1 つの指向性に設定して交互に行なわれる。つまり、所定の信号を構成する電波は、無線装置 10 のアンテナ 11 と無線装置 30 のアレーアンテナ 20 との間で時分割復信（TDD）等の同一周波数で送受信する方式により送受信される。
20

従って、アレーアンテナ 20 の指向性を 1 つの指向性に設定して無線装置 10 のアンテナ 11 から無線装置 30 のアレーアンテナ 20 へ所定の信号を構成する電波を送信し、無線装置 30 において電波の強度 I_{1k} を検出した直後に、同じ
25 所定の信号を構成する電波を無線装置 30 のアレーアンテナ 20 から無線装置 10 のアンテナ 11 へ送信し、無線装置 10 において電波の強度 I_{2k} を検出することができる。その結果、無線装置 10, 30 間において同じ伝送路特性を確保して所定の信号を構成する電波を無線装置 10, 30 間で送受信でき、電波の可

逆性により電波の強度 $I_{11} \sim I_{1n}$ をそれぞれ電波の強度 $I_{21} \sim I_{2n}$ に一致させることができる。そして、無線装置 10 において作成される秘密鍵 K_{s1} を無線装置 30 において作成される秘密鍵 K_{s2} に容易に一致させることができる。

- 5 また、所定の信号を構成する電波は、無線装置 10, 30 間で時分割復信 (TDD) 等の同一周波数で送受信する方式により送受信されるので、電波の干渉を抑制して 1 つのアレーアンテナ 20 を介して所定の信号を構成する電波を無線装置 10, 30 間で送受信できる。

- 10 更に、アレーアンテナ 20 の指向性を 1 つの指向性に設定して無線装置 10, 30 間で所定の信号を構成する電波を送受信し、秘密鍵 K_{s1} , K_{s2} を作成するための受信信号プロファイル $RSSI_1$, $RSSI_2$ を生成するので、図 1 に示すようにアレーアンテナ 20 を装着した無線装置 30 の近傍に盗聴装置 50 が配置されていても、盗聴装置 50 による秘密鍵 K_{s1} , K_{s2} の盗聴を抑制できる。

- 15 即ち、盗聴装置 50 は、アンテナ 11 及びアレーアンテナ 20 から送信された電波をアンテナ 51 を介して受信するが、アレーアンテナ 20 は指向性を各指向性に設定して電波を送受信するので、アンテナ 11 とアレーアンテナ 20 との間で送受信される電波は、アンテナ 11 またはアレーアンテナ 20 とアンテナ 51 との間で送受信される電波と異なり、盗聴装置 50 は、無線装置 30 が送受信する電波と同じ電波を送受信できず、電波の強度 I_{1k} と同じ強度を得ることができない。その結果、盗聴装置 50 は、秘密鍵 K_{s1} , K_{s2} を盗聴することができない。
- 20

- 25 従って、この発明においては、電氣的に指向性を切換え可能なアレーアンテナ 20 を盗聴装置 50 の近傍に配置された無線装置 30 に装着することを特徴とする。

更に、鍵確認用データ $DCFM_1 \sim 4$ は、秘密鍵 K_{s1} , K_{s2} に非可逆的な演算、または一方向的な演算を施して発生されるので、鍵確認用データ $DCFM_1 \sim 4$ が盗聴されても秘密鍵 K_{s1} , K_{s2} が解読される危険性を極めて低くできる。

更に、シンδροーム s_1 , s_2 は、秘密鍵 K_{s1} , K_{s2} のビットパターンを示す鍵 x_1 , x_2 に検査行列 H の転置行列 H^T を乗算して得られるので、シンδροーム s_1 , s_2 が盗聴されても直ちに情報のビットパターンが推測されることは特殊な符号化を想定しない限り起こらない。従って、盗聴を抑制して秘密鍵を一致させることができる。

なお、無線装置 10, 30 間で通信を行なう動作は、実際には、CPU (Central Processing Unit) によって行なわれ、無線装置 10 に搭載された CPU は、図 8 に示す各ステップ S3, S6, S10, S11, S13, S15 を備えるプログラムを ROM (Read Only Memory) から読出し、無線装置 30 に搭載された CPU は、図 8 に示す各ステップ S1, S2, S4, S5, S7, S8, S9, S12, S14, S16 を備えるプログラムを ROM から読出し、無線装置 10, 30 に搭載された 2 つの CPU は、その読出したプログラムを実行して図 8 に示すフローチャートに従って無線装置 10, 30 間で通信を行なう。

従って、ROM は、無線装置 10, 30 間で通信を行なう動作をコンピュータ (CPU) に実行させるためのプログラムを記録したコンピュータ (CPU) 読取り可能な記録媒体に相当する。

そして、図 8 に示す各ステップを備えるプログラムは、アレーアンテナ 20 の指向性を複数個に順次変えて受信した複数の電波に基づいて、無線装置 10, 30 間における通信をコンピュータ (CPU) に実行させるプログラムである。

上記においては、電氣的に指向性を切換え可能なアレーアンテナ 20 を無線装置 30 のみに装着すると説明したが、この発明においては、アレーアンテナ 20 は、無線装置 10 及び 30 の両方に装着されてもよい。

即ち、この発明においては、アレーアンテナ 20 は、2 つの無線装置 10, 30 のうち、少なくとも一方の無線装置に装着されていればよい。そして、アレーアンテナ 20 を装着した無線装置は、好ましくは、盗聴装置 50 の近傍に配置される。

また、この発明においては、秘密鍵 K_{s1} , K_{s2} の鍵長は、無線装置 10, 30 間の通信環境に応じて決定されてもよい。即ち、無線装置 10, 30 間の通

信環境が盗聴し易い環境であるとき、秘密鍵 $Ks1$ 、 $Ks2$ の鍵長を相対的に長くし、無線装置10、30間の通信環境が盗聴しにくい環境であるとき、秘密鍵 $Ks1$ 、 $Ks2$ の鍵長を相対的に短くする。

更に、定期的に秘密鍵 $Ks1$ 、 $Ks2$ の鍵長を変えるようにしてもよい。

- 5 更に、無線装置10、30間で送受信する情報の機密性に応じて秘密鍵 $Ks1$ 、 $Ks2$ の鍵長を変えるようにしてもよい。即ち、情報の機密性が高いとき秘密鍵 $Ks1$ 、 $Ks2$ の鍵長を相対的に長くし、情報の機密性が低いとき秘密鍵 $Ks1$ 、 $Ks2$ の鍵長を相対的に短くする。

- 10 そして、この鍵長は、アレーアンテナ20の指向性を変化させる個数、即ち、制御電圧セット $CLV1 \sim CLVn$ の個数により制御される。秘密鍵 $Ks1$ 、 $Ks2$ は、検出された電波の強度 $I11 \sim I1n$ 、 $I21 \sim I2n$ の個数からなるビットパターンを有し、電波の強度 $I11 \sim I1n$ 、 $I21 \sim I2n$ の個数は、アレーアンテナ20の指向性を変化させる個数に等しいからである。つまり、制御電圧セット $CLV1 \sim CLVn$ の個数により秘密鍵 $Ks1$ 、 $Ks2$ の鍵長を制
15 御できる。

このように、この発明においては、秘密鍵 $Ks1$ 、 $Ks2$ の鍵長は、電氣的に指向性を切換え可能なアレーアンテナ20の指向性を変化させる個数によって決定される。

- 20 更に、上記においては、2つの無線装置間において秘密鍵を生成する場合、即ち、1つの無線装置が1つの無線装置と通信する場合について説明したが、この発明は、これに限らず、1つの無線装置が複数の無線装置と通信する場合についても適用される。この場合、1つの無線装置は、通信の相手毎にアレーアンテナ20の指向性の切換パターンを変えて秘密鍵を生成する。1つの無線装置は、アレーアンテナ20の指向性の切換パターンを1つに固定して複数の無線装置との
25 間で秘密鍵を生成することも可能であるが（複数の無線装置の設置場所によって1つの無線装置との伝送路が異なるので、通信の相手毎に異なる秘密鍵を生成できる）、盗聴を効果的に抑制するには、通信の相手毎にアレーアンテナ20の指向性の切換パターンを変えて秘密鍵を生成するのが好ましい。

〔実施の形態2〕

図9は、実施の形態2による無線通信システムの概略図である。無線通信システム200は、図1に示す無線通信システム100の無線装置10、30をそれぞれ無線装置10A、30Aに代えたものであり、その他は、無線通信システム100と同じである。

5 無線装置10Aには、アンテナ11が装着され、無線装置30Aには、アレーアンテナ20が装着される。無線装置10Aは、無線LAN (Local Area Network) のプロトコルであるIEEE802.11bまたはIEEE802.11gに従って無線装置30Aとの間で通信を行なう。

10 図10は、図9に示す一方の無線装置10Aの内部構成を示す概略ブロック図である。無線装置10Aは、無線装置10の信号発生部10を信号発生部110Aに代えたものであり、その他は、無線装置10と同じである。

信号発生部110Aは、秘密鍵を生成するときに無線装置30Aへ送信するための所定の信号を生成し、その生成した所定の信号を送信処理部120へ出力する。送信処理部120は、暗号部200から暗号化データを受けると、その受け
15 た暗号化データに対して変調、周波数変換および増幅等を施してアンテナ部130から送信する。

なお、実施の形態2においては、送信処理部120は、信号発生部110Aから所定の信号を受けると、所定の信号を所定の通信プロトコルであるIEEE802.11b (またはIEEE802.11g) の物理層を構成するデータフ
20 ーマットに含め、変調、周波数変換および増幅等を施してアンテナ部130から送信する。

図11は、図9に示す他方の無線装置30Aの内部構成を示す概略ブロック図である。無線装置30Aは、無線装置30の信号発生部110を信号発生部110Aに代え、指向性設定部230を指向性設定部230Aに代えたものであり、
25 その他は、無線装置30と同じである。信号発生部110Aについては、上述したとおりである。

実施の形態2においては、アンテナ部220は、送信処理部120からの信号を指向性設定部230Aによって設定された無指向性または指向性で無線装置10Aへ送信する。すなわち、アンテナ部220は、オムニアンテナまたは指向性

アンテナとして機能し、送信処理部 120 からの信号を無線装置 10A へ送信する。また、アンテナ部 220 は、無線装置 10A からの信号を指向性設定部 230A によって設定された指向性で受信して受信処理部 140 またはプロファイル生成部 150 へ出力する。

- 5 指向性設定部 230A は、アンテナ部 220 の指向性を設定する機能を持ち、無線装置 10A、30A において秘密鍵 K_{s1} 、 K_{s2} を生成するとき、後述する方法により、所定の順序に従ってアンテナ部 220 の指向性を順次切換え、またはアンテナ部 220 を無指向性に設定する。

10 図 12 は、図 11 に示す指向性設定部 230A の機能ブロック図である。指向性設定部 230A は、指向性設定部 230 の制御電圧発生回路 231 を制御電圧発生回路 231A に代えたものであり、その他は、指向性設定部 230 と同じである。

指向性設定部 230A は、制御電圧セット $CLV_1 \sim CLV_n$ (n は自然数) を順次発生し、その発生した制御電圧セット $CLV_1 \sim CLV_n$ をバラクタダイオード 232 へ順次出力する。バラクタダイオード 232 は、制御電圧セット $CLV_1 \sim CLV_n$ に応じて無給電素子であるアンテナ素子 21~23, 25~27 に装荷される容量を変え、アレーアンテナ 20 をオムニアンテナまたは指向性アンテナとして機能させる。すなわち、バラクタダイオード 232 は、制御電圧セット $CLV_1 \sim CLV_n$ に応じて無給電素子 21~23, 25~27 のリアクタンス値を変えることによってアレーアンテナ 20 をオムニアンテナまたは指向性アンテナとして機能させる。この場合、制御電圧セット $CLV_1 \sim CLV_n$ の全てが 0V からなるとき、アレーアンテナ 20 は、オムニアンテナとして機能する。そして、バラクタダイオード 232 は、制御電圧セット $CLV_1 \sim CLV_n$ の複数の異なるセットに応じて、無給電素子 21~23, 25~27 のリアクタンス値を順次変え、アレーアンテナ 20 の指向性を複数個に順次変える。

図 13 は、所定の通信プロトコルである IEEE 802.11b (または IEEE 802.11g) の物理層および MAC (Media Access Control) 層のフォーマットを示す図である。物理層は、データを電気信号に変換し、実際の伝送を行なう階層である。そして、物理層は、IEEE 802.

11bおよびIEEE 802.11gの両方に共通なデータフォーマットからなる。また、MAC層は、各無線装置間で信頼性の高いデータ伝送を行なう階層である。物理層は、PLCP (Physical Layer Convergence Protocol) プリアンブルと、PLCPヘッダとからなる。

5 PLCPプリアンブルは、SYNC (SYNChronization field) 信号と、SFD (Start Frame Delimeter) 信号とからなる。また、PLCPヘッダは、SIGNAL (SIGNAL or data rate) 信号と、SERVICE信号と、LENGTH信号と、CRC (Cyclic Redundancy Code) 信号とからなる。

10 SYNC信号は、128ビットのデータ長を有する信号であり、同期の確立に使用される。SFD信号は、16ビットのデータ長を有する信号であり、PLCPプリアンブルの終了を示す。

SIGNAL信号は、8ビットのデータ長を有する信号であり、MAC層のデータ速度を示す。SERVICE信号は、8ビットのデータ長を有する信号であり、機能拡張用として予約されている。LENGTH信号は、16ビットのデータ長を有する信号であり、MAC層のデータ長を示す。CRC信号は、16ビットのデータ長を有する信号であり、誤り検出に用いられる。

15 また、MAC層は、PSDU (PLCP Service Data Unit) からなる。そして、PSDUは、48ビット以上のデータ長を有するMAC層のデータである。

実施の形態2においては、秘密鍵 K_{s1} 、 K_{s2} を生成する場合、無線装置10A、30Aは、所定のデータを物理層に含め、アレーアンテナ20の指向性を変化させながら送信する。より具体的には、SYNC信号、SFD信号、SIGNAL信号、SERVICE信号、LENGTH信号およびCRC信号のうち、
25 SYNC信号、SFD信号、SIGNAL信号およびSERVICE信号を複数のデータ $D_0 \sim D_{11}$ から構成する。そして、複数のデータ $D_1 \sim D_{11}$ は、所定のデータを分割したデータである。

データ D_0 は、36ビットのデータ長を有する。また、複数のデータ $D_1 \sim D_{11}$ の各々は、11ビットのデータ長を有する。11ビットのデータ長に相当す

る時間長を期間T0とすると、複数のデータD1～D11の各々は、3ビットのデータ長に相当する期間T1と、8ビットのデータ長に相当する期間T2とに分割される。

5 秘密鍵Ks1, Ks2を生成する場合、データD0のデータ長に相当する期間T3、アレーアンテナ20をオムニアンテナとして機能させ、データD1～D11全体のデータ長に相当する期間T4、アレーアンテナ20を指向性アンテナとして機能させ、LENGTH信号およびCRC信号のデータ長に相当する期間T5、アレーアンテナ20をオムニアンテナとして機能させて所定のデータを送信する。

10 そして、期間T4においてアレーアンテナ20を指向性アンテナとして機能させる場合、アレーアンテナ20の指向性が順次切換えられる。より具体的には、複数のデータD1～D11の各々の期間T1においてアレーアンテナ20の指向性が変化され、期間T2において、その変化された指向性でデータが送信される。従って、図13に示す例においては、アレーアンテナ20の指向性が11回変更
15 されて所定のデータが送信される。

所定のデータを受信する場合、所定のデータの送信時と同じように、期間T3, T5においてアレーアンテナ20をオムニアンテナとして機能させ、期間T4においてアレーアンテナ20を指向性アンテナとして機能させる。そして、所定のデータの受信時においては、複数のデータD1～D11の各々の期間T1においてアレーアンテナ20の指向性が変化され、その変化された指向性で受信した電
20 波の強度が期間T2において検出される。従って、図13に示す例においては、所定のデータの受信時においても、アレーアンテナ20の指向性は、11回変更される。

25 なお、期間T3においてアレーアンテナ20をオムニアンテナとして機能させるのは、通信の初期においては、AGC (Auto Gain Control) 機能を働かせ、データの受信レベルを最適値に調整する必要があるからである。また、期間T5においてアレーアンテナ20をオムニアンテナとして機能させるのは、次の理由による。物理層およびMAC層のデータ受信に誤りが生じると、確認応答 (=ACK信号) が返らず、再送状態が続いてしまう。したがって、

これを防止するためにMAC層のデータに関連するLENGTH信号および物理層のデータ受信の成否を判定するCRC信号をオムニアンテナで送受信することにしたものである。

5 図14は、2つの無線装置10A、30A間でデータを送受信する通常の方法の概念図である。また、図15は、2つの無線装置10A、30A間におけるデータの再送の概念図である。更に、図16は、この発明の実施の形態において、2つの無線装置10A、30A間でデータを送受信する方法の概念図である。

通常の方法においては、無線装置30Aは、アレーアンテナ20の指向性を指向性パターン(1)に従って順次切換えて所定のデータDAを無線装置10Aへ
10 送信する。そして、無線装置10Aは、所定のデータDAの受信を確認すると、確認応答ACKを無線装置30Aへ送信し、無線装置30Aは、アレーアンテナ20の指向性を指向性パターン(1)に従って順次切換えて確認応答ACKを受信する。その後、無線装置30Aは、アレーアンテナ20の指向性を指向性パターン(2)に従って順次切換えて所定のデータDAを無線装置10Aへ送信する。
15 そして、無線装置10Aは、無線装置30Aから所定のデータDAを受信する(図14参照)。

しかし、このような通常の方法においては、アレーアンテナ20の指向性の変更によって図13に示すSYNC信号以降のデータを誤って受信した場合、物理層の同期は成立しているが、MAC層より上位の層の同期が成立しないため、確認
20 応答ACKが返送されず、図15に示すように、アレーアンテナ20の指向性を指向性パターン(1)に従って順次切換えて所定のデータDAを再送する動作が継続する。その結果、無線装置10A、30A間において双方向の通信ができなくなる。

そこで、この発明においては、図16に示す方法で所定のデータDAを送受信
25 する。すなわち、無線装置30Aは、アレーアンテナ20にオムニパターンを設定して所定のデータDAを無線装置10Aへ送信する。つまり、無線装置30Aは、アレーアンテナ20をオムニアンテナとして機能させて所定のデータDAを無線装置10Aへ送信する。

そして、無線装置10Aは、無線装置30Aからの所定のデータDAの受信を

確認すると、確認応答ACKを無線装置30Aへ送信する。無線装置30Aは、アレーアンテナ20の指向性を指向性パターン(1)に従って順次切換えて確認応答ACKを受信する。その後、無線装置30Aは、アレーアンテナ20の指向性を指向性パターン(1)に従って順次切換えて所定のデータDAを無線装置10Aへ送信する。そして、無線装置10Aは、無線装置30Aから所定のデータDAを受信する(図16参照)。

図16に示す方法においては、無線装置30Aは、最初の送信において、通信が確立しているオムニパターンを使用するため、無線装置10Aから確認応答ACKを必ず受信できる。その結果、無線装置10A、30A間における双方向の通信を確保できる。

そして、確認応答ACKは、図13に示す物理層のフォーマットからなるので、無線装置30Aは、アレーアンテナ20の指向性を指向性パターン(1)に従って順次切換えて確認応答ACKを受信するとき、受信した確認応答ACKに含まれる複数のデータD1~D11に対応する複数の電波強度を検出できる。また、無線装置30Aは、確認応答ACKの受信時における指向性パターン(1)を使用してアレーアンテナ20の指向性を順次切換えて所定のデータDAを無線装置10Aへ送信するので、無線装置10Aは、無線装置30Aにおいて検出された複数の電波強度と同じ複数の電波強度を検出できる。

図16に示す方法によって所定のデータを無線装置10A、30A間で1回送受信した場合、無線装置10A、30Aは、11個の電波強度からなる強度プロファイルPI11, PI21をそれぞれ検出する。そして、無線装置10A、30A間における所定のデータの送受信をm(mは自然数)回繰返すことによって、無線装置10A、30Aは、m個の強度プロファイルPI11~PI1m, PI21~PI2mをそれぞれ検出する。

そして、強度プロファイルPI11~PI1mの全体に含まれる電波強度は、図7に示すn個の電波強度WI1~WInに等しい。従って、無線装置10A、30A間における所定のデータの1回の送受信によって、n個の電波強度WI1~WInのうちの11個の電波強度WI(i)~WI(i+10)(i=1~n-10)が検出される。

つまり、この発明においては、所定の通信プロトコルである IEEE 802.11b (または IEEE 802.11g) の物理層に所定のデータ DA を含めて無線装置 10A, 30A 間で送受信することを m 回繰り返すことによって n 個の電波強度 W I 1 ~ W I n が検出され、その検出された n 個の電波強度 W I 1 ~ W I n に基づいて秘密鍵 K s 1, K s 2 が生成される。

図 17 は、図 9 に示す 2 つの無線装置 10A, 30A 間で通信を行なう動作を説明するためのフローチャートである。一連の動作が開始されると、無線装置 30A の送信処理部 120 は、k = 1 を設定する (ステップ S 21)。そして、指向性設定部 230A は、アレーアンテナ 20 をオムニアンテナとして機能させ、所定のデータ DA を無線装置 10A へ送信する (ステップ S 22)。

続いて、無線装置 10A のアンテナ部 130 は、所定のデータ DA を受信し (ステップ S 23)、その受信した所定のデータ DA を受信処理部 140 へ出力する。そして、受信処理部 140 は、所定のデータ DA の受信を確認すると、送信処理部 120 は、確認応答 (ACK 信号) をアンテナ部 130 から無線装置 30A へ送信する (ステップ S 24)。

無線装置 30A の指向性設定部 230A は、アンテナ部 220 をオムニアンテナ、指向性アンテナおよびオムニアンテナとして順次機能させ、アンテナ部 220 は、確認応答 (ACK 信号) を受信する (ステップ S 25)。すなわち、アレーアンテナ 20 は、図 13 に示すデータ D 0 をオムニアンテナとして受信し、指向性をパターン P k により 11 個に変化させながらデータ D 1 ~ D 11 を受信し、更に、LENGTH 信号および CRC 信号をオムニアンテナとして受信する。

そして、アンテナ部 220 は、受信した複数のデータ D 1 ~ D 11 に対応する複数の電波をプロファイル生成部 150 へ出力する。プロファイル生成部 150 は、アンテナ部 220 からの複数の電波の強度プロファイル P I 1 k を検出する (ステップ S 26)。

次に、無線装置 30A の信号発生部 110A は、所定のデータを発生して送信処理部 120 へ出力し、送信処理部 120 は、所定のデータを物理層のデータ D 1 ~ D 11 に割り当て、オムニアンテナ、指向性アンテナおよびオムニアンテナとして順次機能させたアンテナ部 220 を介して無線装置 10A へ所定のデータ

を送信する（ステップS27）。すなわち、アンテナ部220は、図13に示すデータD0をオムニアンテナとして送信し、指向性をパターンPkにより11個に変化させながらデータD1～D11を送信し、更に、LENGTH信号およびCRC信号をオムニアンテナとして送信する。

5 無線装置10Aにおいて、アンテナ部130は、無線装置30Aから所定のデータを受信する。（ステップS28）。そして、アンテナ部130は、受信した複数のデータD1～D11に対応する複数の電波をプロファイル生成部150へ出力する。プロファイル生成部150は、アンテナ部130からの複数の電波の強度プロファイルPI2kを検出する（ステップS29）。

10 その後、無線装置30Aの送信処理部120は、 $k = k + 1$ を設定し（ステップS30）、 $k = m$ であるか否かを判定する（ステップS31）。そして、 $k = m$ でないとき、ステップS22～S31が繰返し実行される。即ち、アレーアンテナ20の指向性パターンがパターンP1～Pmによってm個に変えられて、無線装置10Aのアンテナ部130と無線装置30Aのアンテナ部220との間で
15 所定のデータを構成する電波が送受信され、強度プロファイルI11～I1m及びI21～I2mが検出されるまで、ステップS2～S11が繰返し実行される。

ステップS11において、 $k = m$ であると判定されると、無線装置30Aにおいて、プロファイル生成部150は、強度プロファイルI11～I1mに含まれる強度I11～I1nから受信信号プロファイルRSSI1を作成して鍵作成部
20 160へ出力する。

鍵作成部160は、受信信号プロファイルRSSI1から最大強度WImax1を検出し、その検出した最大強度WImax1によって受信信号プロファイルRSSI1を規格化し、強度I11～I1nを多値化する。そして、鍵作成部160は、多値化した各値をビットパターンとする秘密鍵Ks2を生成する（ステ
25 ップS32）。

また、無線装置10Aのプロファイル生成部150は、強度プロファイルI21～I2mに含まれる強度I21～I2nから受信信号プロファイルRSSI2を作成して鍵作成部160へ出力する。鍵作成部160は、受信信号プロファイルRSSI2から最大強度WImax2を検出し、その検出した最大強度WIm

a x 2によって受信信号プロファイルRSSI 2を規格化し、強度I 21～I 2nを多値化する。そして、鍵作成部160は、多値化した各値をビットパターンとする秘密鍵K s 1を生成する（ステップS 33）。

5 ステップS 34～ステップS 39は、図8に示すフローチャートのステップS 14～ステップS 19と同じである。

10 上述したステップS 22～S 24に示す動作は、アレーアンテナ20をオムニアンテナとして機能させて無線装置10Aと無線装置30Aとの間で通信を確立する動作である。また、ステップS 24～S 26に示す動作は、無線装置30Aにおいて受信信号プロファイルRSSI 1を生成するための電波を無線装置10Aのアンテナ11から無線装置30Aのアレーアンテナ20へ送信し、かつ、無線装置30Aにおいて電波の強度プロファイルPI 1kを検出する動作であり、ステップS 27～S 29に示す動作は、無線装置10Aにおいて受信信号プロファイルRSSI 2を生成するための電波を無線装置30Aのアレーアンテナ20から無線装置10Aのアンテナ11へ送信し、かつ、無線装置10Aにおいて電波の強度プロファイルPI 2kを検出する動作である。そして、所定のデータを構成する電波の無線装置10Aのアンテナ11から無線装置30Aのアレーアンテナ20への送信及び所定のデータを構成する電波の無線装置30Aのアレーアンテナ20から無線装置10Aのアンテナ11への送信は、アレーアンテナ20の指向性をパターンP kに従って変えながら交互に行なわれる。つまり、所定のデータを構成する電波は、無線装置10Aのアンテナ11と無線装置30Aのアレーアンテナ20との間で時分割通信により送受信される。

25 従って、アレーアンテナ20の指向性をパターンP kに従って変えながら無線装置10Aのアンテナ11から無線装置30Aのアレーアンテナ20へ所定のデータを構成する電波を送信し、無線装置30Aにおいて電波の強度プロファイルPI 1kを検出した直後に、同じ所定のデータを構成する電波を無線装置30Aのアレーアンテナ20から無線装置10Aのアンテナ11へ送信し、無線装置10Aにおいて電波の強度プロファイルPI 2kを検出することができる。その結果、無線装置10A、30A間において同じ伝送路特性を確保して所定のデータを構成する電波を無線装置10A、30A間で送受信でき、電波の可逆性により

電波の強度 $I_{11} \sim I_{1n}$ をそれぞれ電波の強度 $I_{21} \sim I_{2n}$ に一致させることができる。そして、無線装置 10A において作成される秘密鍵 K_{s1} を無線装置 30 において作成される秘密鍵 K_{s2} に容易に一致させることができる。

5 また、所定のデータを構成する電波は、無線装置 10A、30A 間で時分割通信により送受信されるので、電波の干渉を抑制して 1 つのアレーアンテナ 20 を介して所定のデータを構成する電波を無線装置 10A、30A 間で送受信できる。

更に、所定のデータは、所定の通信プロトコルである IEEE 802.11b および IEEE 802.11g に共通な物理層に含めて無線装置 10A、30A 間で送受信されるので、通信プロトコルが IEEE 802.11b から IEEE 802.11g へ変化してもデータフォーマットを変えずに秘密鍵 K_{s1} 、 K_{s2} を生成できる。

更に、無線装置 30A は、無線装置 10A からの確認応答 (ACK 信号) の受信時および所定のデータの無線装置 10A への送信時、同じパターン P_k によってアレーアンテナ 20 の指向性を順次変更する (ステップ S25, S27 参照)。
15 そして、同じパターン P_k によってアレーアンテナ 20 の指向性を順次変更して無線装置 10A から確認応答 (ACK 信号) を受信する動作 (ステップ S25) および所定のデータを無線装置 10A へ送信する動作 (ステップ S27) は、 $k = m$ になるまで繰返し実行されるので、ステップ S25, S27 において、パターン P_k に従ってアレーアンテナ 20 の指向性を順次変更することは、アレーアンテナ 20 の指向性を更新して無線装置 10A から確認応答 (ACK 信号) を受信し、その更新した指向性を維持して所定のデータを無線装置 10A へ送信することに相当する。
20

このように、図 16 に示す方法によって所定のデータを無線装置 10A、30A 間で送受信することによって所定のデータの再送が繰返されるのを防止し、無線装置 10A、30A 間における双方向の通信を確保できる。すなわち、無線装置 10A、30A において同じ秘密鍵 K_{s1} 、 K_{s2} を安定して作成できる。
25

更に、アレーアンテナ 20 の指向性をパターン P_k に従って変えながら無線装置 10A、30A 間で所定のデータを構成する電波を送受信し、秘密鍵 K_{s1} 、 K_{s2} を作成するための受信信号プロファイル $RSSI_1$ 、 $RSSI_2$ を生成す

るので、図9に示すようにアレーアンテナ20を装着した無線装置30Aの近傍に盗聴装置50が配置されていても、盗聴装置50による秘密鍵 K_{s1} 、 K_{s2} の盗聴を抑制できる。

5 即ち、盗聴装置50は、アンテナ11及びアレーアンテナ20から送信された電波をアンテナ51を介して受信するが、アレーアンテナ20は指向性をパターン P_k に従って変えながら電波を送受信するので、アンテナ11とアレーアンテナ20との間で送受信される電波は、アンテナ11またはアレーアンテナ20とアンテナ51との間で送受信される電波と異なり、盗聴装置50は、無線装置30Aが送受信する電波と同じ電波を送受信できず、電波の強度プロファイル P_{I1k} と同じ強度プロファイルを得ることができない。その結果、盗聴装置50は、
10 秘密鍵 K_{s1} 、 K_{s2} を盗聴することができない。

従って、この発明においては、電氣的に指向性を切換え可能なアレーアンテナ20を盗聴装置50の近傍に配置された無線装置30Aに装着することを特徴とする。

15 更に、鍵確認用データ $DCFM1 \sim 4$ は、秘密鍵 K_{s1} 、 K_{s2} に非可逆的な演算、または一方向的な演算を施して発生されるので、鍵確認用データ $DCFM1 \sim 4$ が盗聴されても秘密鍵 K_{s1} 、 K_{s2} が解読される危険性を極めて低くできる。

更に、シンδροーム $s1$ 、 $s2$ は、秘密鍵 K_{s1} 、 K_{s2} のビットパターンを示す鍵 x_1 、 x_2 に検査行列 H の転置行列 H^T を乗算して得られるので、シンδροーム $s1$ 、 $s2$ が盗聴されても直ちに情報のビットパターンが推測されることは
20 特殊な符号化を想定しない限り起こらない。従って、盗聴を抑制して秘密鍵を一致させることができる。

なお、無線装置10A、30A間で通信を行なう動作は、実際には、CPUによって行なわれ、無線装置10Aに搭載されたCPUは、図17に示す各ステップ $S23$ 、 $S24$ 、 $S28$ 、 $S29$ 、 $S33$ 、 $S34$ 、 $S36$ 、 $S38$ を備えるプログラムをROMから読出し、無線装置30Aに搭載されたCPUは、図17
25 に示す各ステップ $S21$ 、 $S22$ 、 $S25$ 、 $S26$ 、 $S27$ 、 $S30$ 、 $S31$ 、 $S32$ 、 $S35$ 、 $S37$ 、 $S39$ を備えるプログラムをROMから読出し、無線

装置 10A, 30A に搭載された 2 つの CPU は、その読出したプログラムを実行して図 17 に示すフローチャートに従って無線装置 10A, 30A 間で通信を行なう。

5 従って、ROM は、無線装置 10A, 30A 間で通信を行なう動作をコンピュータ (CPU) に実行させるためのプログラムを記録したコンピュータ (CPU) 読取り可能な記録媒体に相当する。

そして、図 17 に示す各ステップを備えるプログラムは、アレーアンテナ 20 の指向性を複数個に順次変えて受信した複数の電波に基づいて、無線装置 10A, 30A 間における通信をコンピュータ (CPU) に実行させるプログラムである。

10 その他は、実施の形態 1 と同じである。

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

15

産業上の利用可能性

この発明は、秘密鍵の盗聴を抑制可能な無線通信システムに適用される。

請求の範囲

1. 指向性を電氣的に切換え可能な第1のアンテナ(20)と、
第2のアンテナ(11)と、

5 前記第1及び第2のアンテナ(20, 11)を介して無線伝送路により電波を相互に送受信する第1及び第2の無線装置(30, 10)とを備え、

前記第1の無線装置(30)は、前記第1のアンテナ(20)の指向性が所定のパターンにより複数個に変えられたときに前記第2の無線装置(10)から受信した複数の電波に基づいて前記複数の電波の強度プロファイルを示す第1の受信信号プロファイルを生成し、その生成した第1の受信信号プロファイルに基づいて第1の秘密鍵(Ks2)を生成し、

15 前記第2の無線装置(10)は、前記第1のアンテナ(20)の指向性が所定のパターンにより複数個に変えられたときに前記第1の無線装置(30)から受信した複数の電波に基づいて前記複数の電波の強度プロファイルを示す第2の受信信号プロファイルを生成し、その生成した第2の受信信号プロファイルに基づいて前記第1の秘密鍵(Ks2)と同じ第2の秘密鍵(Ks1)を生成する、無線通信システム。

2. 前記第1及び第2の受信信号プロファイルの各々は、前記複数個の指向性に対応した複数の強度からなり、

20 前記第1及び第2の無線装置(30, 10)は、前記複数の強度を多値化してそれぞれ前記第1及び第2の秘密鍵(Ks2, Ks1)を生成する、請求の範囲第1項に記載の無線通信システム。

3. 前記第1及び第2の無線装置(30, 10)は、時分割復信方式により前記複数の電波を送受信する、請求の範囲第1項に記載の無線通信システム。

25 4. 前記第1の無線装置(30)は、前記生成した第1の秘密鍵(Ks2)が前記第2の秘密鍵(Ks1)に一致することを確認する、請求の範囲第1項に記載の無線通信システム。

5. 指向性を電氣的に切換え可能な第1のアンテナ(20)と、
第2のアンテナ(11)と、

前記第 1 及び第 2 のアンテナ (20, 11) を介して無線伝送路により電波を相互に送受信する第 1 及び第 2 の無線装置 (30A, 10A) とを備え、

5 前記第 1 の無線装置 (30A) は、前記第 1 のアンテナ (20) の指向性が所定のパターンにより複数個に変えられたときに前記第 2 の無線装置 (10A) が所定の通信プロトコルに従って送信した複数のデータに対応する複数の電波を受信し、その受信した複数の電波に基づいて前記複数の電波の強度プロファイルを示す第 1 の受信信号プロファイルを生成し、その生成した第 1 の受信信号プロファイルに基づいて第 1 の秘密鍵 (Ks2) を生成し、

10 前記第 2 の無線装置 (10A) は、前記第 1 のアンテナ (20) の指向性が所定のパターンにより複数個に変えられたときに前記第 1 の無線装置 (30A) が前記所定の通信プロトコルに従って送信した複数のデータに対応する複数の電波を受信し、その受信した複数の電波に基づいて前記複数の電波の強度プロファイルを示す第 2 の受信信号プロファイルを生成し、その生成した第 2 の受信信号プロファイルに基づいて前記第 1 の秘密鍵 (Ks2) と同じ第 2 の秘密鍵 (Ks1) を生成する、無線通信システム。

20 6. 前記第 1 の無線装置 (30A) は、前記第 1 のアンテナ (20) が無指向性に制御されたときに前記第 2 の無線装置 (10A) との間で前記無線伝送路を確立し、前記無線伝送路が確立した後、前記第 1 のアンテナ (20) の指向性を前記複数個に変えながら前記第 2 の無線装置 (10A) との間で前記複数のデータを送受信する、請求の範囲第 5 項に記載の無線通信システム。

25 7. 前記第 1 の無線装置 (30A) は、前記第 2 の無線装置 (10A) との間における前記各データの送受信において、前記第 1 のアンテナ (20) の指向性を更新して前記第 2 の無線装置 (10A) から前記データを受信し、前記更新した前記第 1 のアンテナ (20) の指向性を維持して前記受信したデータを前記第 2 の無線装置 (10A) へ送信する、請求の範囲第 6 項に記載の無線通信システム。

8. 前記所定の通信プロトコルは、複数の階層からなり、

前記複数のデータは、前記複数の階層のうち、前記データを前記電気信号に変換する階層におけるデータフォーマットに含まれ、

前記データを前記電気信号に変換する階層は、複数の通信プロトコルに共通な

階層である、請求の範囲第 6 項に記載の無線通信システム。

9. 前記複数のデータの各々は、前記第 1 および第 2 の無線装置 (30A, 10A) により受信された電波の強度を検出する区間と、前記第 1 のアンテナ (20) の指向性を変更する区間とからなる、請求の範囲第 5 項に記載の無線通信システム。

10. 前記第 1 の無線装置 (30, 30A) は、前記生成した第 1 の秘密鍵 (Ks2) が前記第 2 の秘密鍵 (Ks1) に不一致であるとき、前記第 1 の秘密鍵 (Ks2) を前記第 2 の秘密鍵 (Ks1) に一致させる、請求の範囲第 1 項から請求の範囲第 9 項のいずれか 1 項に記載の無線通信システム。

11. 前記第 1 のアンテナ (20) は、盗聴者の端末 (50) に近接して配置された第 1 の無線装置 (30, 30A) に設置される、請求の範囲第 1 項から請求の範囲第 9 項のいずれか 1 項に記載の無線通信システム。

12. 前記第 1 及び第 2 の無線装置 (30, 30A, 10, 10A) は、前記第 1 及び第 2 の秘密鍵 (Ks2, Ks1) を用いてデータを暗号及び復号して相互に通信する、請求の範囲第 1 項から請求の範囲第 9 項のいずれか 1 項に記載の無線通信システム。

FIG. 1

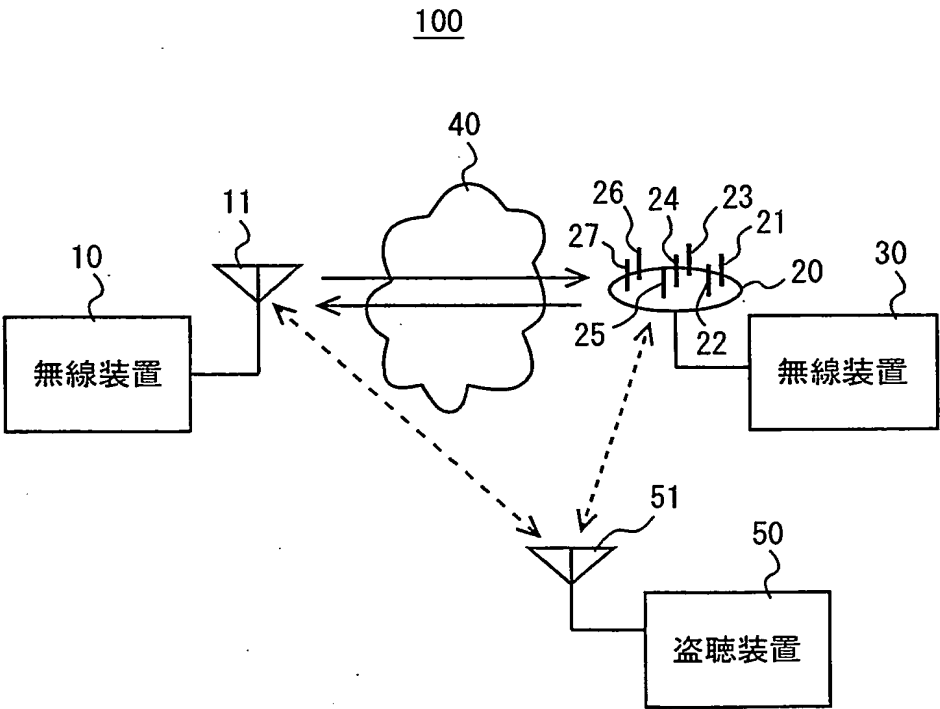


FIG. 2

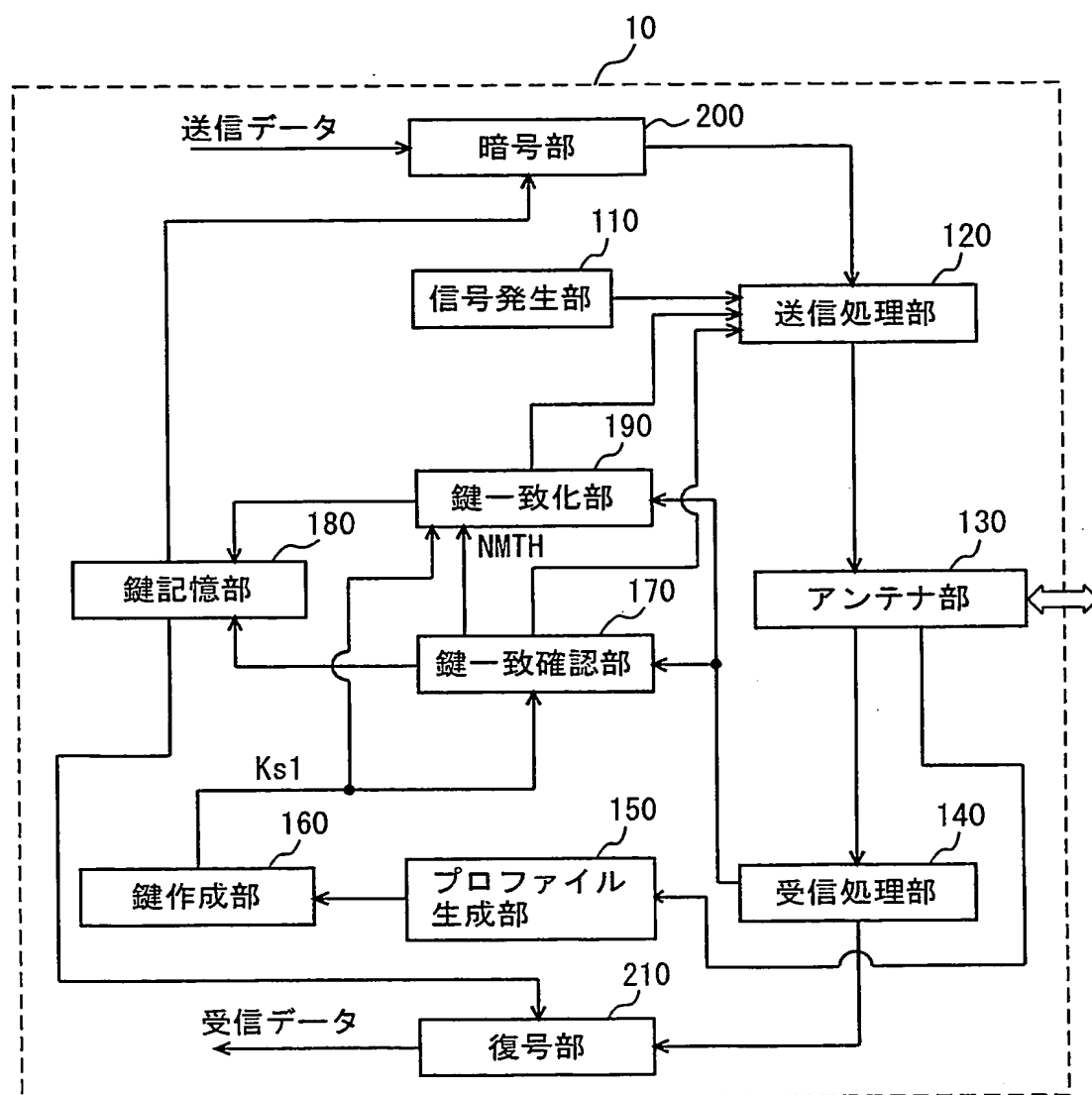


FIG. 3

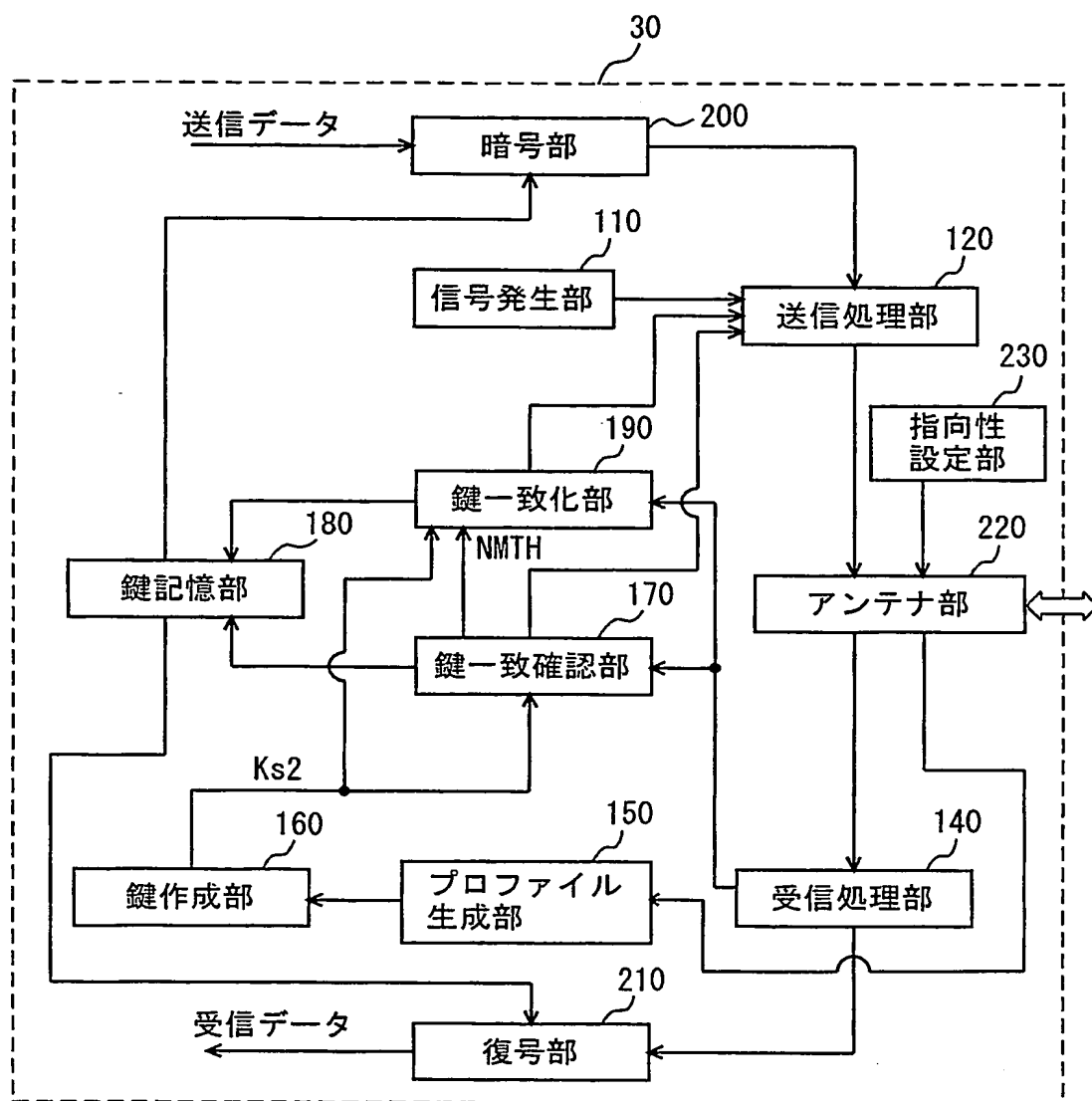


FIG. 4

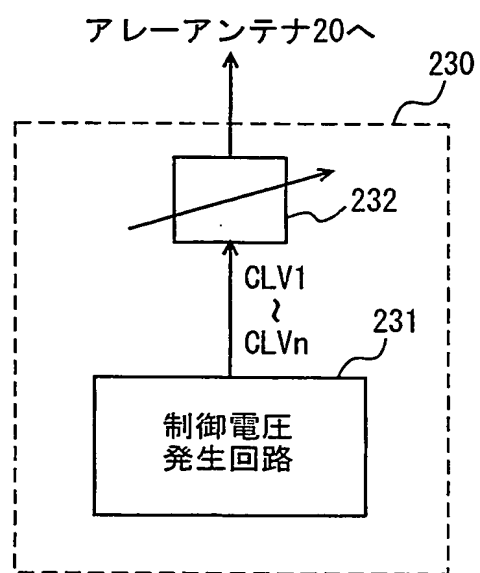


FIG. 5

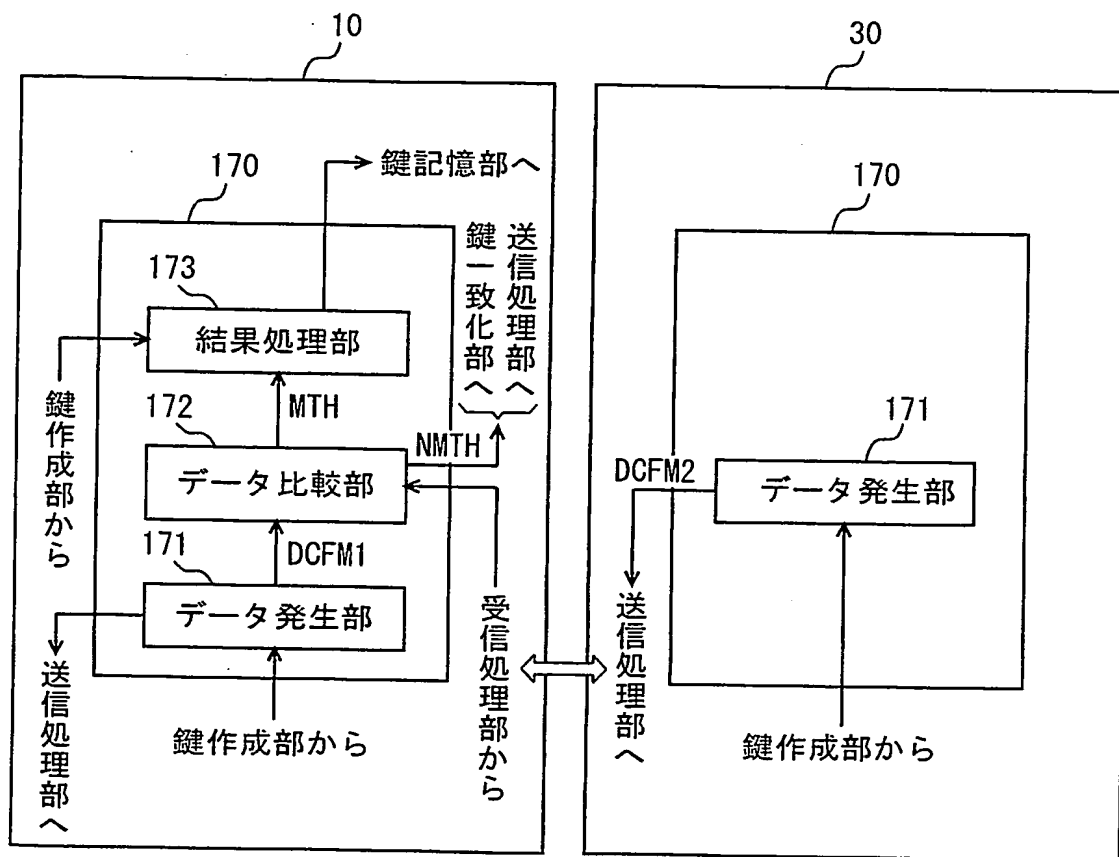


FIG. 6

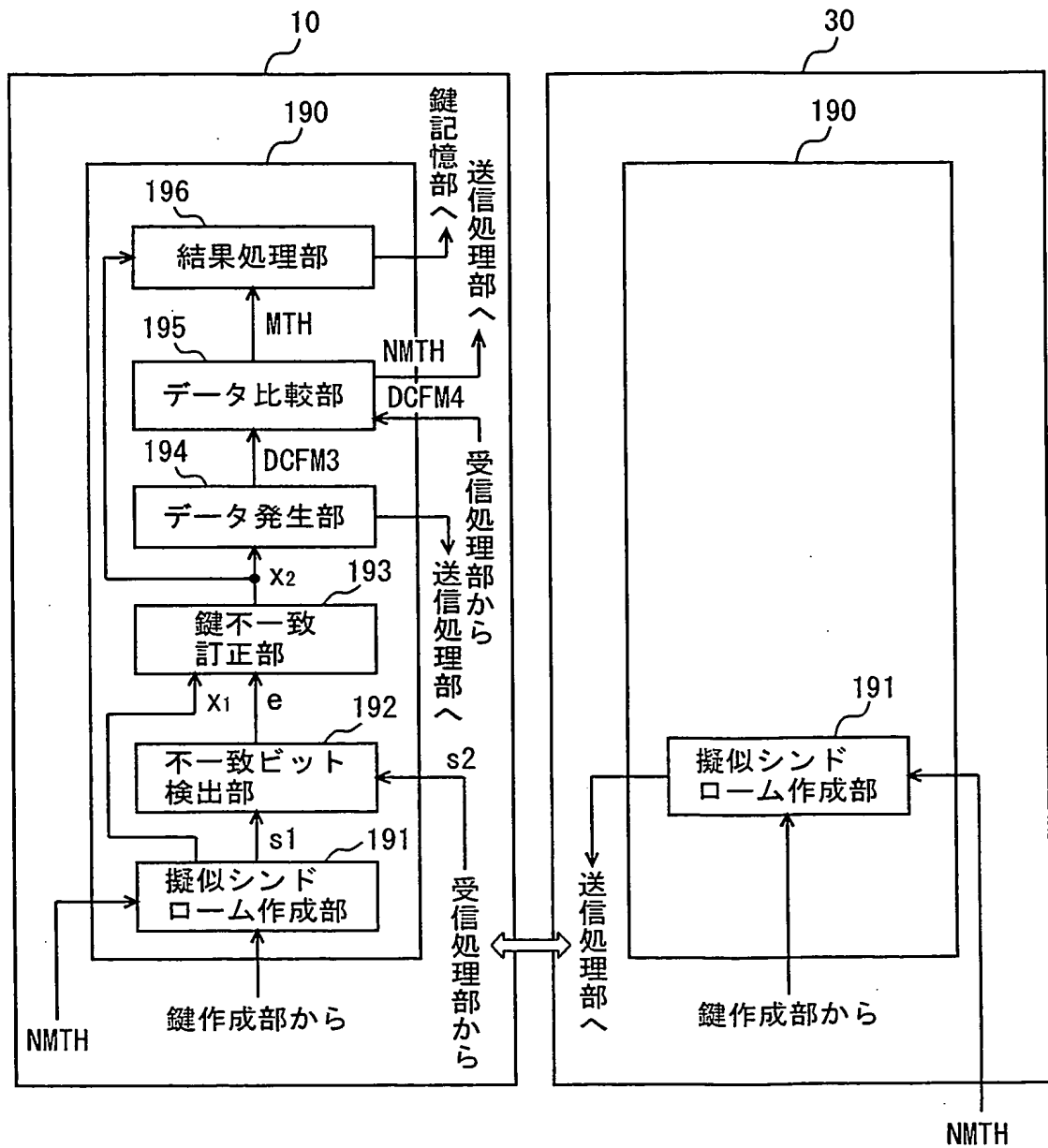
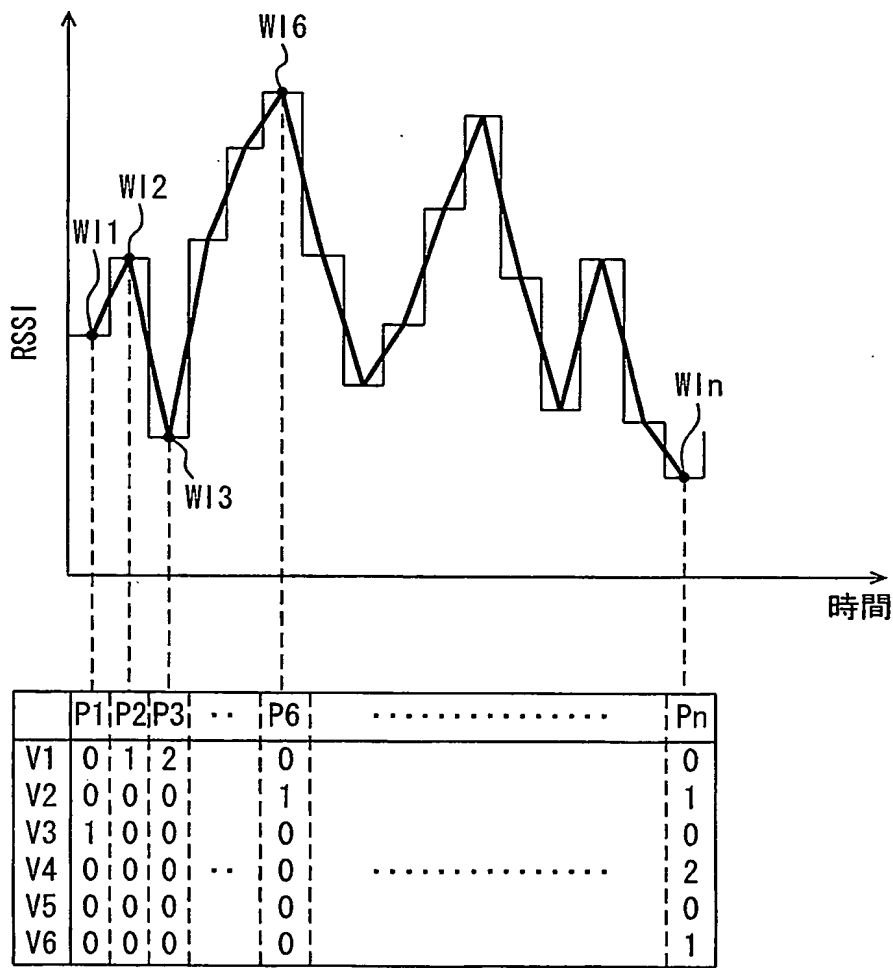


FIG. 7



FI G ∞

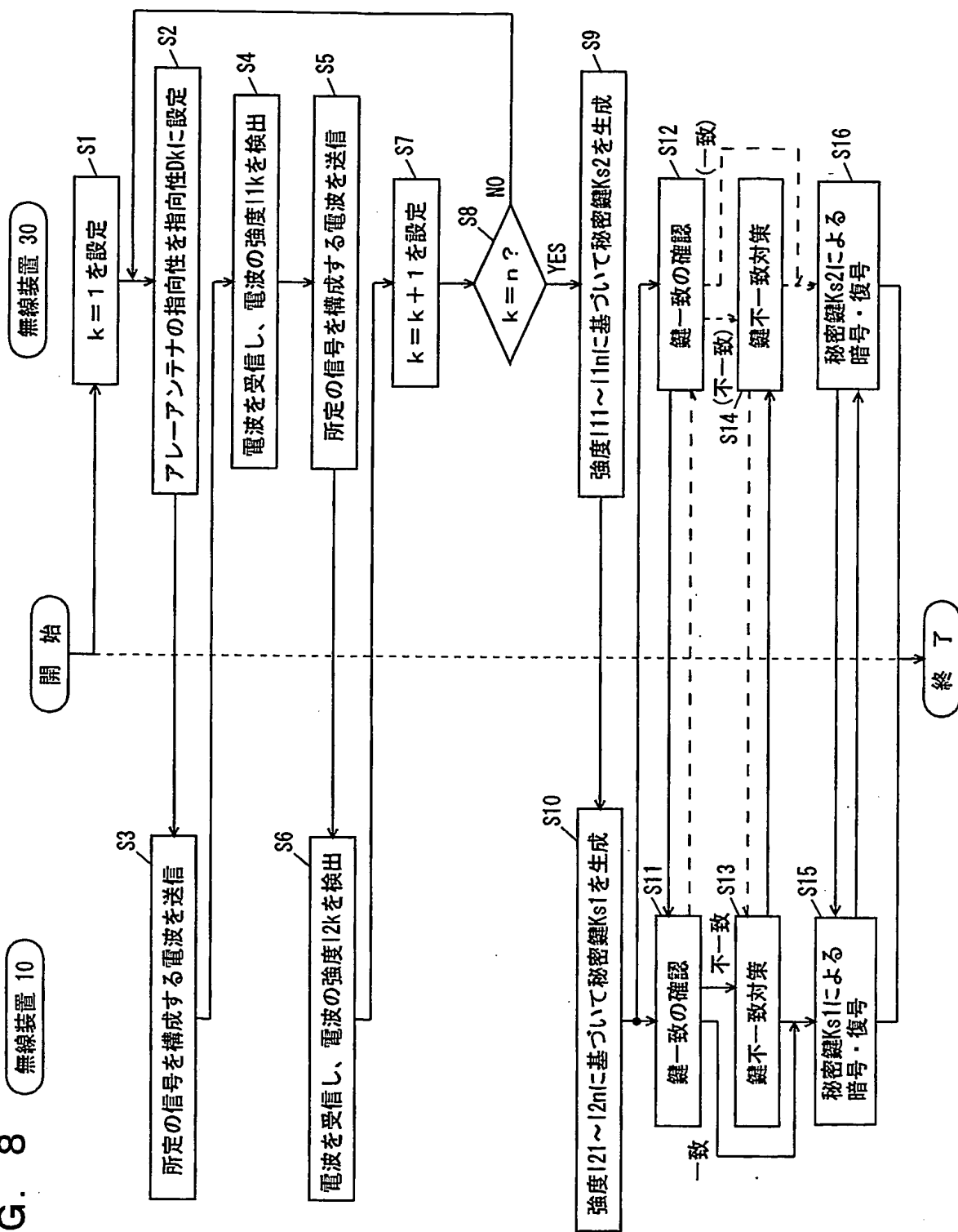


FIG. 9

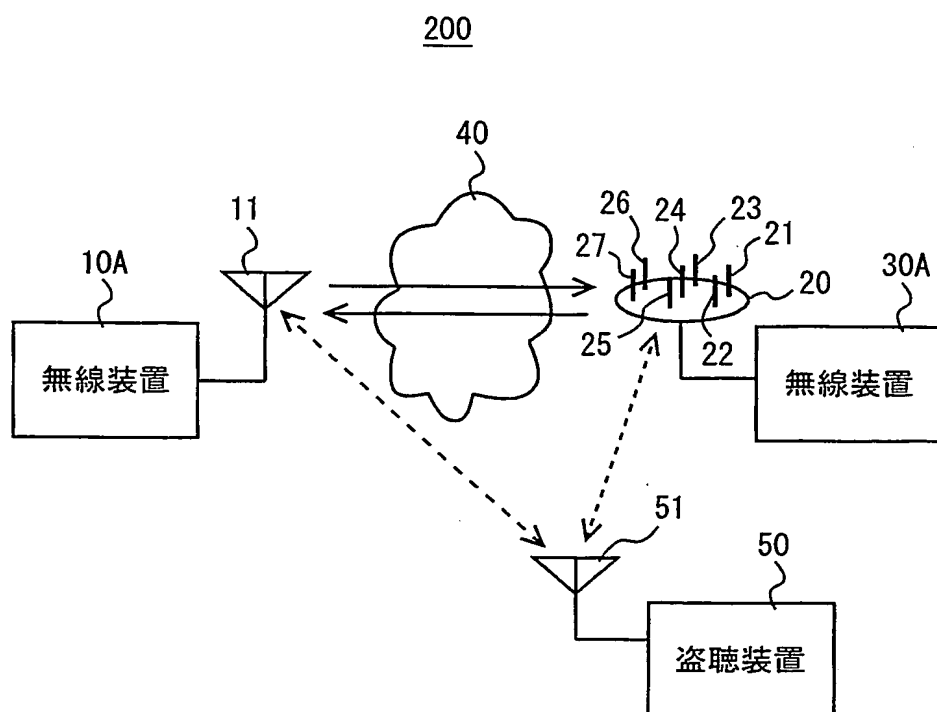


FIG. 10

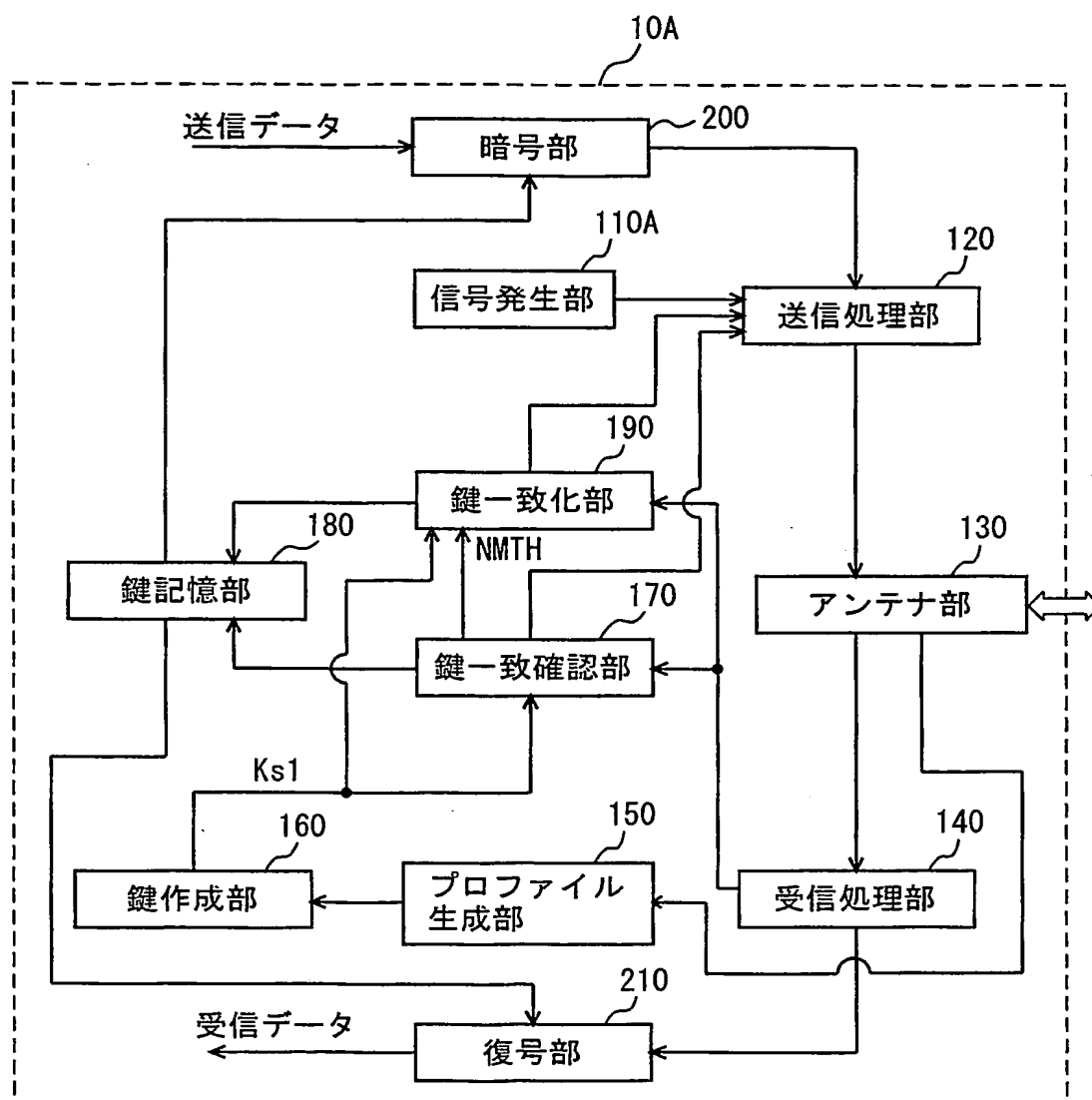


FIG. 11

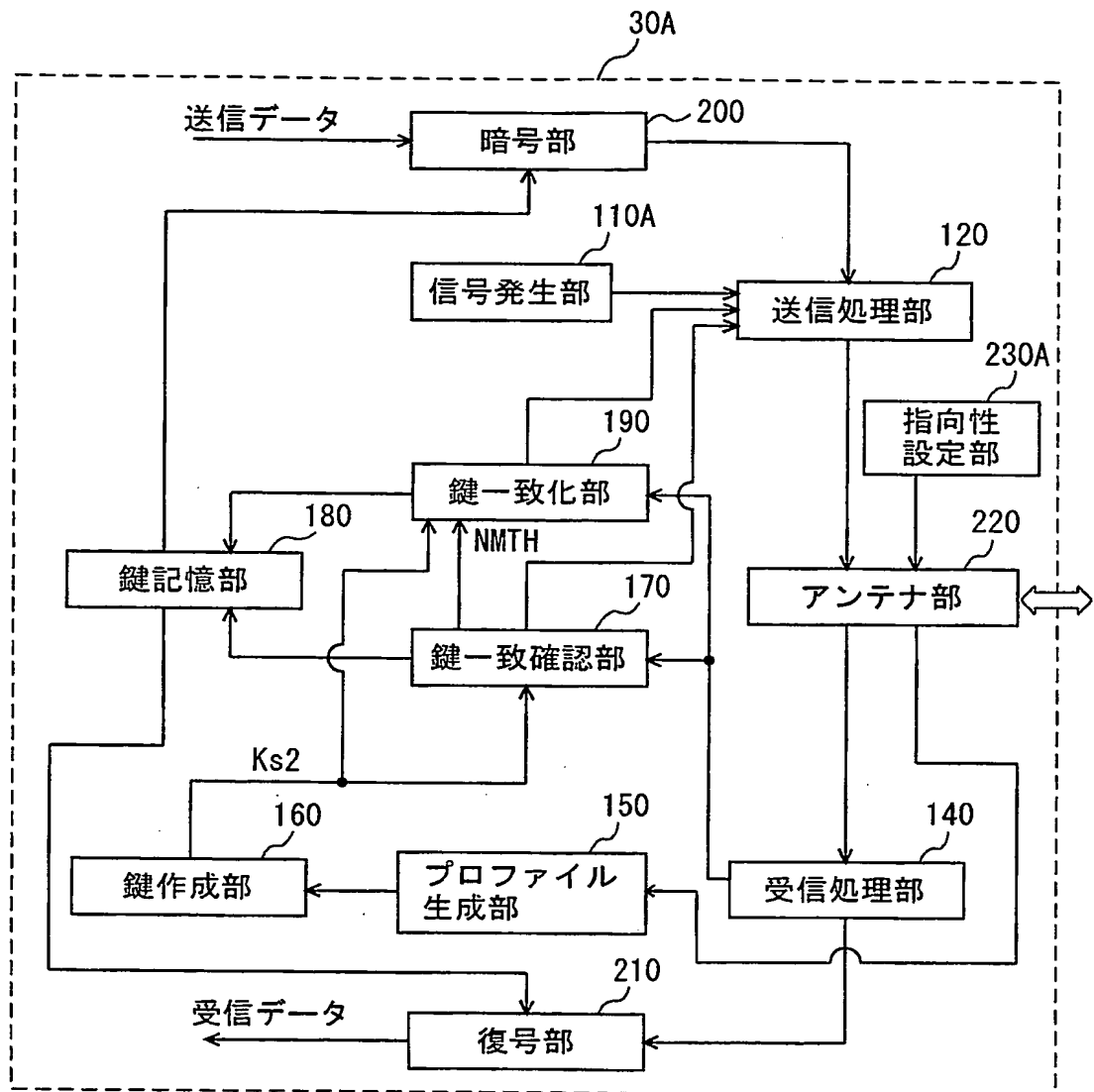


FIG. 12

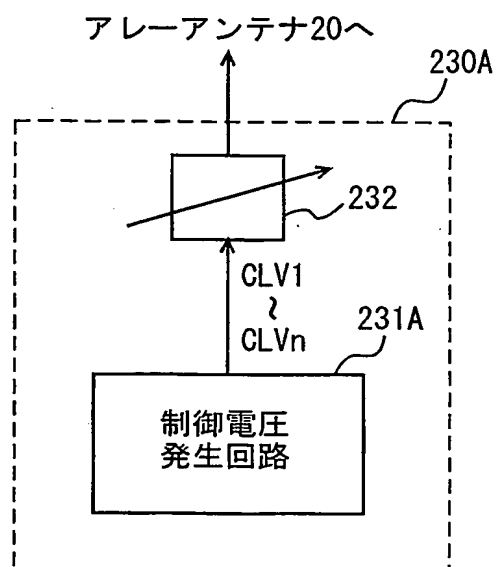


FIG. 13

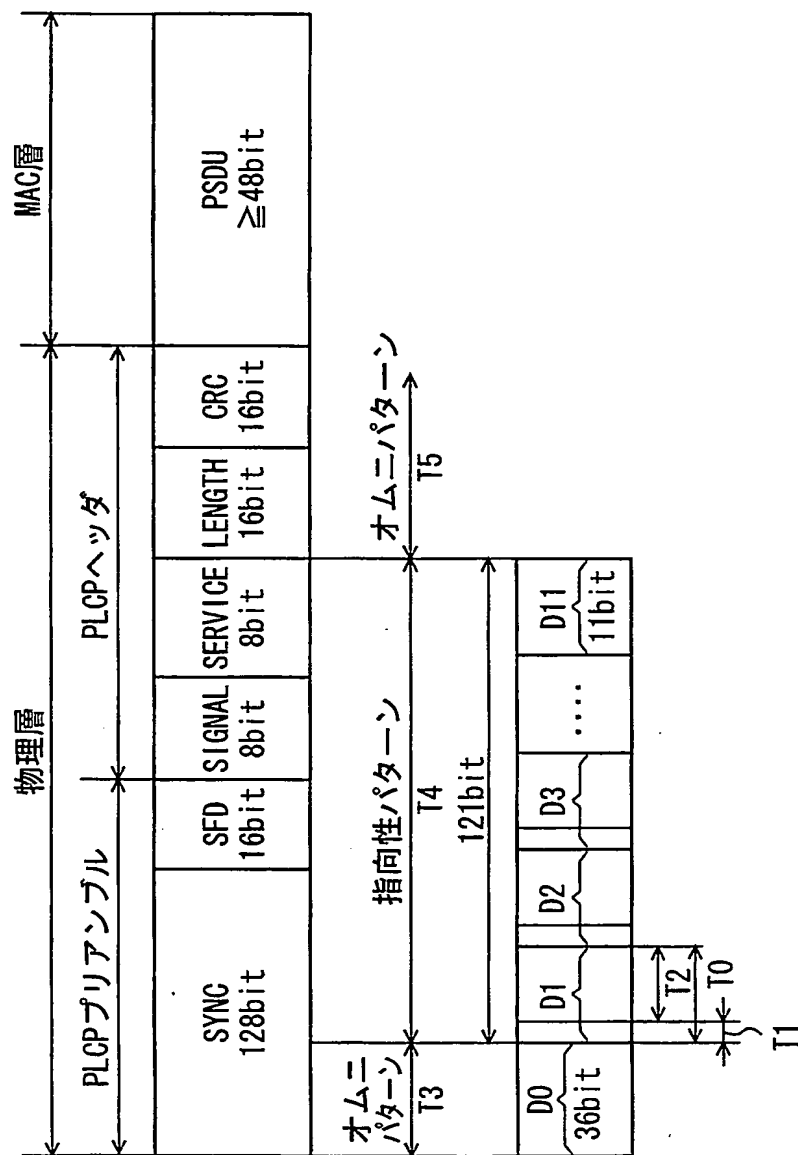


FIG. 14

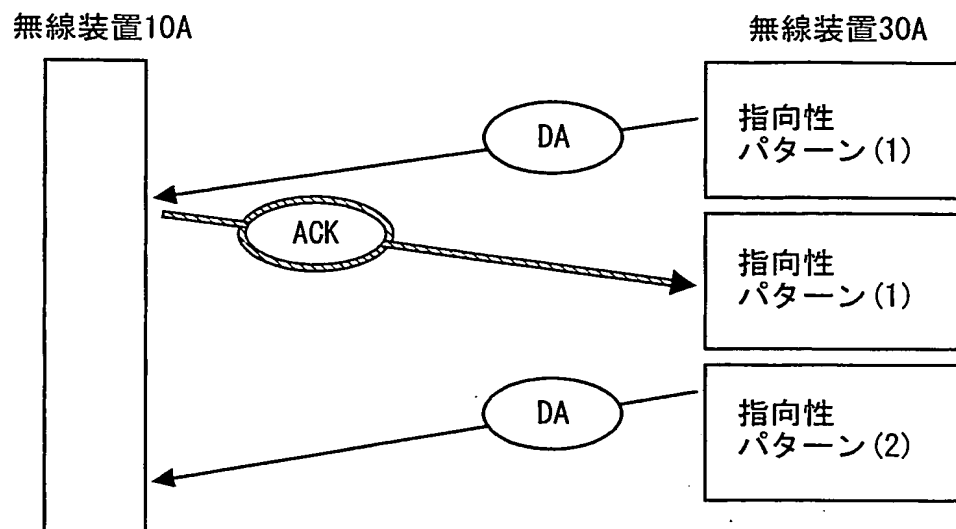


FIG. 15

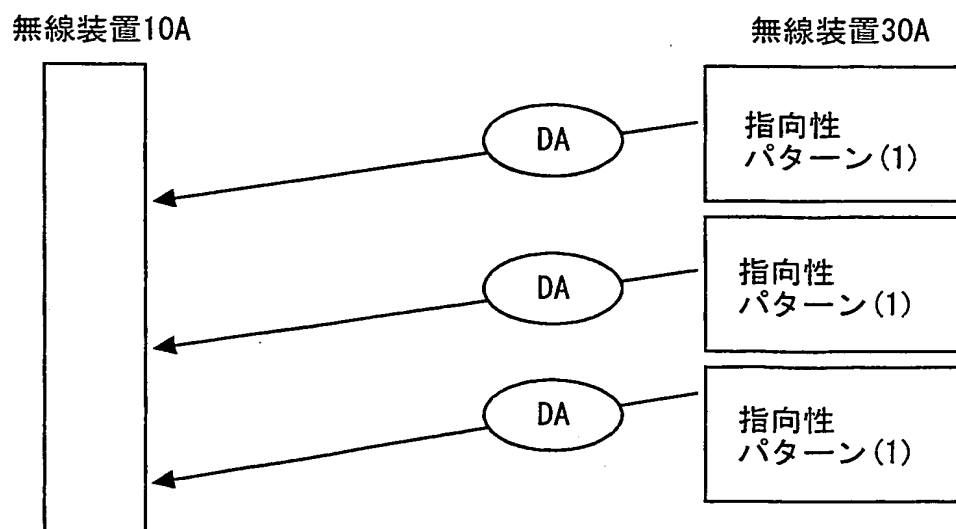


FIG. 16

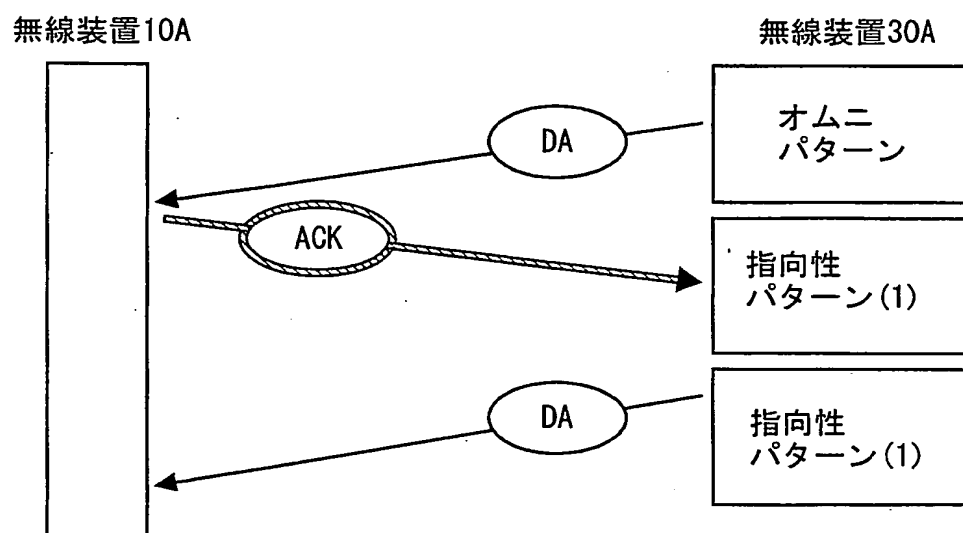
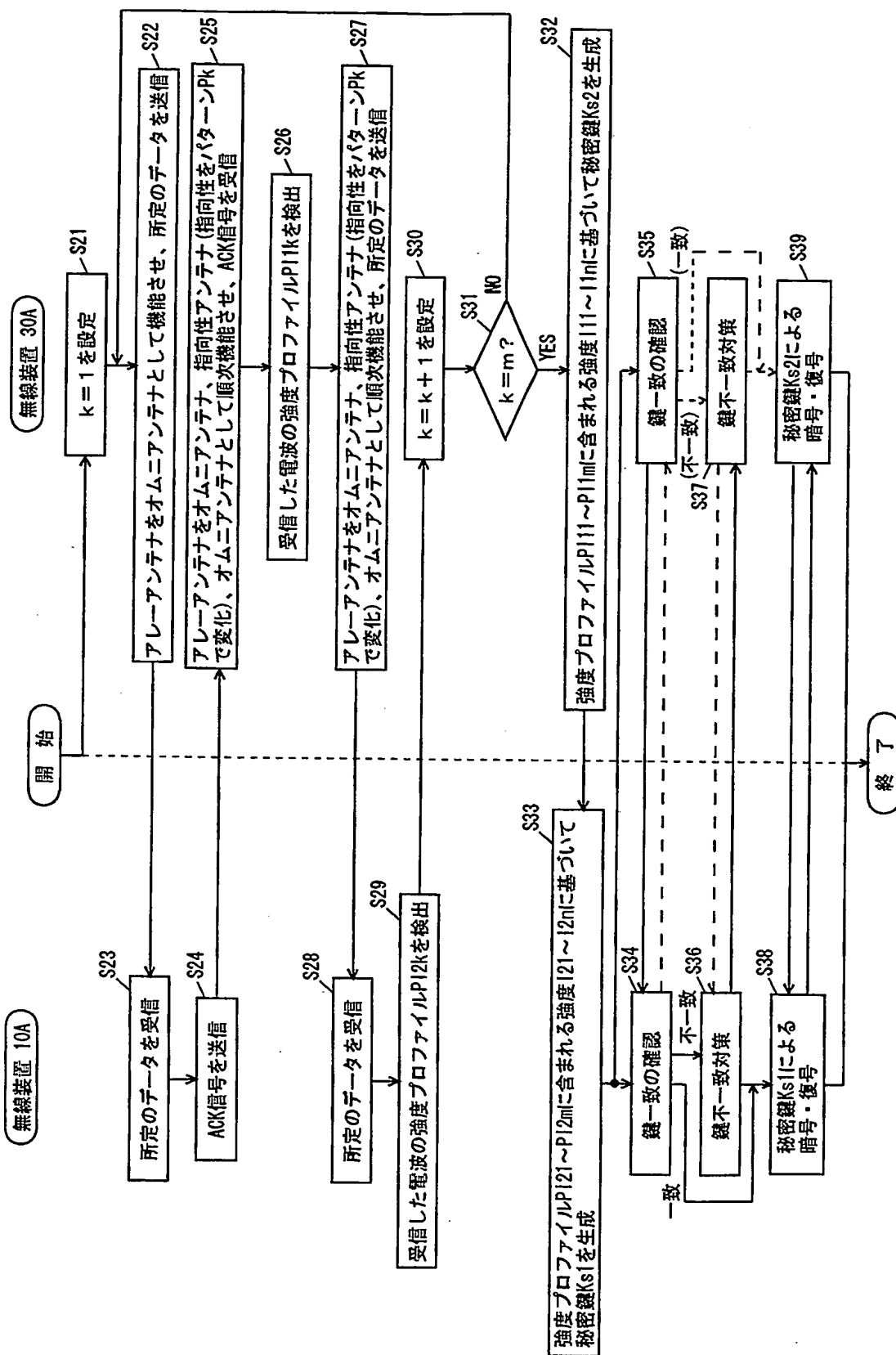


FIG. 17



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/002228

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L9/08, H04K1/00, H04Q7/38, H04M1/725, H04B7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁷ H04L9/08, H04K1/00, H04Q7/38, H04M1/725, H04B7/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2002-152191 A. (Matsushita Electric Industrial Co., Ltd.), 24 May, 2002 (24.05.02), Par. Nos. [0321] to [0354]; Figs. 29 to 34 (Family: none)	1-12
Y	Hideichi Motoki HORIIKE, Hideichi SASAOKA, "Rikujo Ido Tsushinro no Fukisoku Hendo ni Motozuku Himitsu Kagi Kyoyu Hoshiki", The Institute of Electronics, Information and Communication Engineers Gijutsu Kenkyu Hokoku, RCS2002-172 to 180, 11 October, 2002 (11.10.02), Vol.102, No.374, pages 7 to 12	1-12

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
17 May, 2004 (17.05.04)

Date of mailing of the international search report
01 June, 2004 (01.06.04)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/002228

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 5-233326 A (Sharp Corp.), 18 May, 1993 (18.05.93), Full text; Figs. 1 to 7 (Family: none)	6
E, X	JP 2004-32679 A (Matsushita Electric Industrial Co., Ltd.), 29 January, 2004 (29.01.04), Full text; all drawings (Family: none)	1-12

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl.⁷ H04L9/08, H04K1/00, H04Q7/38, H04M1/725,
H04B7/10

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl.⁷ H04L9/08, H04K1/00, H04Q7/38, H04M1/725,
H04B7/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2004年
日本国登録実用新案公報	1994-2004年
日本国実用新案登録公報	1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P 2002-152191 A (松下電器産業株式会社) 2002.05.24 第【0321】-【0354】段落、図29-34 (ファミリーなし)	1-12
Y	堀池元樹, 笹岡秀一: “陸上移動通信路の不規則変動に基づく秘密 鍵共有方式” 電子情報通信学会技術研究報告RCS2002-172~180, 2002.10.11, Vol. 102, No. 374 p. 7-12	1-12

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

- 「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

- 「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

17.05.2004

国際調査報告の発送日

01.6.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)
郵便番号100-8915
東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳

5M

4229

電話番号 03-3581-1101 内線 3597

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	JP 5-233326 A (シャープ株式会社) 1993. 05. 18 全文, 図1-7 (ファミリーなし)	6
E, X	JP 2004-32679 A (松下電器産業株式会社) 2004. 01. 29 全文, 全図 (ファミリーなし)	1-12